ONP Command-Line Reference

Intel Networking Division

Revision: ONS SMC 1.2
April 2014

LEGAL

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm.

Intel and Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

* Other names and brands may be claimed as the property of others.

Copyright © 2014, Intel Corporation. All Rights Reserved.

Contents

Revisions ... 11

1. Introduction ... 12

- **1.1 Overview ... 12**
- **1.2 About this Document ... 12**
- **1.3 Acronyms ... 13**

2. Accessing the ONP Platform ... 14

- **2.1 Connecting to the Switch Console Port ... 14**
  - 2.1.1 Console Port Pinout ... 14
  - 2.1.1 Console Console Port Settings ... 14
- **2.2 Setting the Management IP Address ... 15**
- **2.3 Accessing the CLI Using the Console Port ... 15**
- **2.4 Accessing the CLI Using SSH ... 16**
- **2.5 Accessing Wind River Linux Using SSH ... 16**

3. About ONP Configuration Methods ... 17

- **3.1 Manual Configuration using the CLI ... 17**
- **3.2 Programmatically with API Calls ... 17**
- **3.3 Programmatically with CLI Calls ... 17**
- **3.4 SNMP ... 17**

4. About the CLI ... 18

- **4.1 Access Levels ... 18**
- **4.2 Getting Context-Sensitive Help ... 18**
- **4.3 Command Conventions ... 19**
- **4.4 Command Syntax ... 20**
  - 4.4.1 Parameter Value Conventions ... 20
  - 4.4.2 About Show Commands ... 20
  - 4.4.2.1 Show Filtering ... 20
  - 4.4.3 Comments ... 22
- **4.5 Command Shortcuts ... 22**
- **4.6 Keyboard Shortcuts ... 22**
- **4.7 The no Command ... 23**
- **4.8 CLI Severity Messages ... 24**
- **4.9 Command Modes ... 24**
- **4.10 Navigating Command Modes ... 25**
- **4.11 About the CLI Reference Chapters ... 27**
  - 4.11.1 CLI Command Fields ... 27

4.12 Saving ONP Configuration Changes 27
4.13 Restoring ONP Configuration 28
4.13.1 Restoring the Saved Configuration 28
4.13.2 Restoring the Default Configuration 28
4.14 Viewing the Current Configuration 28
4.15 Platform Default Configuration 34
4.16 System Logs 34
4.17 Core Files 35
5. Platform Commands 36
5.1 User Execution Mode Commands 36
show cpu 36
show memory 37
show disk 38
show disk performance 39
5.2 Privileged Mode Commands 41
clear config 41
clear statistics 41
copy 43
cpu threshold 43
delete file 45
dir 45
disk performance threshold 45
disk threshold 47
exit 48
memory threshold 48
reload 49
restore config 50
save config 50
show applications 51
show cpu 53
show disk 54
show disk performance 55
show environment 56
show interface mgmt-ethernet 59
show logging 61
show memory 61
show ntp-associations 62

show radius-server 63
show saved-configs 64
show snmp 64
show snmp group 65
show snmp user 65
show snmp host 66
show snmp community 68
show snmp view 68
show software-upgrade state 69
show tacacs-server 69
show usersname 70
snmp-server chassis-id 71
snmp-server community 71
snmp-server contact 72
snmp-server description 72
snmp-server group 73
snmp-server host 75
snmp-server location 76
snmp-server user 77
snmp-server view 78
software config-data 78
software upgrade start 79
software upgrade load 79
software upgrade cancel 80
software upgrade commit 80

5.3 Global Configuration Mode Commands..82

interface mgmt-ethernet 82
logging application level 82
logging host transport 83
logging host syslog 86
ntp peer 88
ntp server 89
password 90
radius-server 90
tacacs-server 91
username authentication 91

5.4 Management Port Interface Mode 93
duplex 93
ip default-gateway 93
hostname 94
ip address 94
mtu 94
shutdown 95
speed 95
threshold metric 96
6. Layer 2 Commands 98
6.1 User Mode Commands 98
show interface (User) 98
show mac-address-table (User) 99
show mac-address-table static 99
show monitor 100
show terminal 101
show version 101
show vlan 101
terminal length 102
6.2 Privileged Mode Commands 104
clear mac-address-table 104
delete saved-config 104
vlan-database 105
show access-groups 106
show access-lists 106
show access-lists policers 108
show channel-group 109
show clock 111
show dcb app 111
show dcb cn 112
show dcb dcbx 113
show dcb ets-conf 115
show dcb ets-reco 116
show dcb pfc 117
show dot1q-tunnel 118
show errdisable 119

show lldp 120
show interface (Privileged) 123
show interface flowcontrol 125
show port-channel 126
show interface port-channel 127
show mac-address-table (Privileged) 129
show mls qos 129
show monitor 130
show multicast 131
show ovs 132
show spanning-tree 133
show spanning-tree interface 134
show spanning-tree mst 137
show system 139
show statistics 140
show storm-control 141
show running-config 143
show tech-support 144
show terminal 144
show ufd 145
show users 148
show vlan (Privileged) 148
terminal length 148
6.3 Global Configuration Mode Commands............ **150**
access-list action 150
access-list arp ip 152
access-list arp request ip 153
access-list arp response ip 154
access-list expression 156
access-list icmp 172
access-list igmp 173
access-list ip 174
access-list mac 175
access-list policer 176
access-list tcp 177
access-list udp 179

auto-shutdown 180
errdisable 180
fan 181
interface (modes) 182
interface port-channel range 183
interface range 183
ip address (config) 184
ip default-gateway (config) 184
ip igmp snooping 185
lacp enable 186
lacp system-priority 186
lldp (config) 187
mac-address-table multicast (config) 187
mac-address-table static (config) 188
mls qos 189
monitor source 190
no interface port-channel 191
ovs bridge 192
ovs bridge controller 192
ovs flow 192
ovs resources rules-limit 194
port-channel 194
power-supply 196
spanning-tree (config) 198
storm-control 200
switch 201
ufd 202
ufd enable 202
ufd recovery-delay 203
vlan (mode) 204
vlan dot1q tag native 204
6.4 Port Interface Configuration Mode Commands 206
access-group (config-if interface) 206
channel-group 206
cut-through 208
dcb 209

encapsulation dot1q 212

[no] encapsulation dot1q <*vlanId*> [<*vlanPriority*>] 212

flowcontrol 212

ip igmp snooping 213

lldp (config-if) 214

mac-address (config-if interface) 216

mac-address-table (config-if) 216

mls qos map cos-bandwidth 217

mls qos trust 217

ovs port add 218

priority-queue 218

shutdown (port) 219

spanning-tree (config-if interface) 219

spanning-tree mst (config-if interface) 221

speed (config-if interface) 223

storm-control (config-if interface) 223

switchport (config-if interface) 225

ufd group (config-if) 227

ufd group (config-if-range) 227

wrr-queue 228

6.5 VLAN Interface Configuration Mode Commands....230

vlan 230

6.6 Port Channel Interface Configuration Mode Commands....231

access-group (config-if, port-channel) 231

cut through 231

encapsulation dot1q 232

[no] encapsulation dot1q <*vlanId*> [<*vlanPriority*>] 232

ip igmp 232

key 233

lacp 233

mac-address (config-if, port-channel) 234

mac-address-table learning-mode 234

max-frame-size (config-if, port-channel) 235

name (config-if, port-channel) 236

spanning-tree (config-if, port-channel) 236

spanning-tree mst 238

switchport (config-if, port-channel) 240
ufd group 241
6.7 STP Configuration Mode Commands... 243
instance 243
name (config-mst) 243
revision 244
6.8 VLAN Simple Configuration Mode Commands 245
name (vlan simple) 245
7. Layer 3 Commands 246
7.1 User Mode Commands... 246
ping 246
ping6 246
7.2 Privileged Mode Commands 248
ping 248
ping6 248
show ip igmp snooping 249
show ip name-server 253

Revisions

Rev	Date	Notes
1.2	01/04/14	Created initial version of the ONS SMC 1.2.
1.2	08/04/14	Updated to actual state for ONS SMC 1.2 revision.

1. Introduction

1.1 Overview

The Open Network Platform (ONP) is a modular and user-configurable Ethernet-based switching platform designed to provide OSI Layer 1, Layer 2, and Layer 3 functionality. The software is integrated with a selection of switching silicon chipsets to provide a wide range of platform options.

You manage the ONP software and your network with one or more of the following methods:

- Command-Line Interface (CLI)
- Programmatically with XML-RPC calls or CLI calls
- Simple Network Management Protocol (SNMP)

Each method enables you to configure, manage, and control the software locally or remotely. The management methods are standards-based. The commands and command modes included in a build are based on the included software modules at build-time. The available modules are as follows:

- Main software (mandatory)
- Open vSwitch software module (optional)

  Open vSwitch provides support for standard management interfaces and opens the forwarding functions to programmatic extension and control using the OpenFlow protocol. For more information, see www.openflow.org.

- Layer 3 software module (optional)

  Layer 3 provides network functions associated with logical addressing, network routing, VLANs, encapsulation, fragmentation, and error handling.

1.2 About this Document

This document is for network administrators and operators who configure, manage, and maintain the ONP software. The document provides information on how to access the CLI, how to use the CLI, and how to upgrade the ONP software.

The CLI topics are as follows:

- Accessing the ONP Platform where you will learn how to access the ONP from a direct connection to the platform, from a LAN, and from a remote host.
- About ONP Configuration Methods where you will learn about the available methods to configure the ONP.
- About the CLI where you will learn how to use the CLI, including privilege levels, help functions, command shortcuts, keyboard shortcuts, mode switching methods, and log files.
- Platform Commands provides a description of all platform related CLI commands, their syntax, and example usage.
- Layer 2 Commands provides a description of all layer 2 related CLI commands, their syntax and example usage.
- Layer 3 Commands provides a description of all layer 3 related CLI commands, their syntax, and example usage.
- No Commands provides a description of all the no commands for the platform.
- Command Index provides a list of commands in alphabetical order.

Note: To configure the ONP using CLI commands, refer to the *ONP Configuration Guide*.
Configuration examples and network use cases also form part of the *ONP Configuration Guide*.
To configure the ONP programmatically, refer to the *ONP XML-RPC Reference and User Guide*.

1.3 Acronyms

ABR	Area Border Router
ACL	Access Control List
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CBS	Credit-based Shaper
CLI	Command Line Interface
CNPV	Congestion Notification Priority Value
CoS	Class of Service
DCB	Data Center Bridging
DCBx	Data Center Bridging eXchange
DSCP	Differentiated Services Code Point
ETS	Enhanced Transmission Selection
IGMP	Internet Group Management Protocol
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LLDP	Link Layer Discovery Protocol
LSA	Link State Advertisement
MACsec	IEEE MAC Security standard
MD5	Message-Digest Algorithm
MLS	Multilayer Switching
MTU	Maximum Transmission Unit
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PFC	Priority-based Flow Control
QoS	Quality of Service
RFC	Request for Comments
RSTP	Rapid Spanning Tree Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TLV	Type-length-value
UDP	User Datagram Protocol
VLAN	Virtual local area network.
WRR	Weighted Round Robin

2. Accessing the ONP Platform

2.1 Connecting to the Switch Console Port

2.1.1 Console Port Pinout

The serial console port on the IZ1 platform uses an RJ45 connector (marked "C") at the top right side of the front panel. The serial console port on the Seacliff Trail platform uses an RJ45 connector (marked "C") at the top left side of the front panel.

Table 1-1. Console Port Pinout

IZ1 Console Port Pinout			Seacliff Trail Console Port Pinout		
PIN	**DIR**	**NAME**	**PIN**	**DIR**	**NAME**
1	IN	RTS — request to send	1	IN	DSR — data set ready
2	-	NC — no connection	2	IN	DCD — data carrier detect
3	OUT	TD — transmit data	3	OUT	DTR — data terminal ready
4	GND	Ground	4	GND	Ground
5	GND	Ground	5	IN	RD — receive data
6	IN	RD — receive data	6	OUT	TD — transmit data
7	-	NC — no connection	7	IN	CTS — clear to send
8	IN	CTS — clear to send	8	OUT	RTS — request to send

Note: An RJ45 to DB9 female adapter cable is included with Seacliff Trail.

2.1.1 Console Console Port Settings

The console port is configured by default with the following settings:

- Baud rate: 115200
- Data bits: 8
- Stop bits: 1
- Parity: none
- Flow control: none

2.2 Setting the Management IP Address

By default, the management port is factory set to DHCP.

To set a static IP address for the management port that will come up on every reboot:

1. Login from the console port as admin/admin to access the command line interface.
2. Configure Ethernet (eth0) via the CLI using the following commands:

```
cli> enable
cli# configure
cli (config)# interface mgmt-ethernet
cli (config-if)# ip address x.x.x.x y.y.y.y
(where x.x.x.x is the IP address and y.y.y.y is the subnet)
cli (config-if)# gateway x.x.x.x
cli (config-if)# no shutdown
cli (config-if)# exit
cli (config)# exit
cli# save config
```

2.3 Accessing the CLI Using the Console Port

To login to the switch platform’s CLI using the console port:

- Login at the prompt as **admin**/**admin** (default username and password), for example:

```
ssh admin@<IP address>
admin@128.224.30.98's password:

Connecting ...

Checking application states ...
Checking table states ...
Checking platform information ...
Getting user information ...
Authenticating ...

Switch >
```

2.4 Accessing the CLI Using SSH

To login to the switch platform's CLI as **admin**/**admin** (default username and password):

- Issue the following SSH command from a computer that has a route to the switch's management port (substitute the management IP address you set for a.b.c.d below):

```
ssh admin@a.b.c.d
```

```
admin@a.b.c.d's password:
```

2.5 Accessing Wind River Linux Using SSH

To login to the switch platform's Wind River Linux as **onsadmin**/**onsadmin** (default username and password):

- Issue the following SSH command from a computer that has a route to the switch's management port (substitute the management IP address you set for a.b.c.d below):

```
ssh onsadmin@a.b.c.d
```

```
onsadmin@a.b.c.d's password:
```

3. About ONP Configuration Methods

ONP uses embedded database tables that define the platform configuration. ONP provides a Northbound API that provides access to the tables from the CLI, programmatically with Extensible Markup Language - Remote Procedure Calls (XML-RPCs), or with the Simple Network Management Protocol (SNMP).

3.1 Manual Configuration using the CLI

To configure the platform manually using the CLI you logon to the platform and enter CLI commands from a keyboard.

3.2 Programmatically with API Calls

You can use a programming language to make calls to the ONP Norrthbound API and configure the platform from an application. Your application must call XML-RPC methods in the form of HTTP requests. For information on how to configure ONP using the Northbound API, see the *ONP Application Programmer's Guide*.

3.3 Programmatically with CLI Calls

You can use a programming language to make calls to the CLI and configure the platform from an application. Your application must invoke the CLI programmatically and execute CLI commands from within the application.

3.4 SNMP

You can use a Simple Network Management Protocol (SNMP) utility to manage the platform. With the use of Management Information Bases (MIBs) you can read and modify system parameters.

4. About the CLI

This topic provides information on the implementation of the command-line interface that allows you to manage the ONP from a host using text entry.

For information on how to access the ONP from a host, see Accessing the ONP Platform.

The CLI implementation topics are as follows:

- Access Levels
- Getting Context-Sensitive Help
- Command Conventions
- Command Syntax
- Command Shortcuts
- Keyboard Shortcuts
- The no Command
- Error Messages
- Command Modes
- Navigating Command Modes
- About the CLI Reference Chapters
- Saving ONP Configuration Changes
- Restoring ONP Configuration
- Viewing the Current Configuration
- Platform Default Configuration
- System Logs
- Core Files

4.1 Access Levels

User access and authentication for the ONP CLI is managed by the default Linux login mechanism. The user roles are pre-defined based on the user **id/group** at platform login time.

The following ONP CLI access levels are available:

- **User**: This level allows access to the configuration data with the ability to modify some parameters.

The User mode prompt is as follows:

```
>
```

- **Privileged**: This level allows access to the platform configuration data with the ability to modify all platform parameters. Upon logging-in, an administrator accesses the User privilege mode (>). To access the Privileged mode (#), use the **enable** command at the User mode prompt. For example:

```
>
>enable
#
```

To return to the User mode, enter **exit** or **Ctrl-c**.

To terminate the CLI session and return to the Root mode, enter **exit** or **Ctrl-c** at the User level prompt.

See also, Getting Context-Sensitive Help and Command Modes.

4.2 Getting Context-Sensitive Help

Upon initial access to a CLI session, you are in the **User** mode where the prompt is **>**. For example:

```
>
```

Enter a question mark (**?**) at the command prompt to display help for the specified mode. `Table 4-1` lists the methods to access context-sensitive help.

Table 4-1. Getting Help

Help Command	Description
>?	Displays the top level commands available in the User mode. A brief description of each command is

	included in the output.
#?	Displays the top level commands available in the Privileged mode. A brief description of each command is included in the output.
(*modeName*) #?	Displays the commands and modes available for the current mode. A brief description of each item is included in the output.
(*modeName*) #*commandName*?	Provides a brief description of the command or mode.
>*commandName* ?	Displays the parameters, commands, and modes available for the current mode. A brief description of each item is included in the output. <cr> indicates that the command can be used without additional parameters.
>*commandName parameterName*?	Provides a brief description of the parameter.
>*commandName parameterName* ?	Provides the valid values for the parameter.
>*commandName* + space + Tab	Displays the parameters, commands, and modes available for the current mode.
>*commandName* + space + Tab + Tab	Displays the parameters, commands, and modes available for the current mode. The second Tab redisplays the items with a brief description for each item.

See also, Command Shortcuts.

4.3 Command Conventions

In this document, command names and command options are in **bold**. Placeholders are in *italic*. `Table 4-2` lists the command conventions for parameter values.

Table 4-2. Command Conventions

Symbol	Example	Description
<> Angle brackets	<value>	A parameter value is required.
[] Square brackets	[value]	A parameter value is optional.
| Vertical bar	option1 | option2	Separates the mutually exclusive parameter options.
{} Curly braces	{option1 | option2}	A parameter option is required.
[{}] Braces within square brackets	[{option1 | option2}]	A parameter option is optional.
WORD (all capital letters)	<WORD>	Indicates that you must enter one word.
LINE (all capital letters)	<LINE>	Indicates that you must enter more than one word. All information entered must be surrounded by double quotes. For example, “New hostname”.

4.4 Command Syntax

A command is one or more words that might be followed by one or more parameters and one or more parameter options. You must enter the parameters and parameter values in the specified order. For information on context-sensitive help, see Getting Context-Sensitive Help.

4.4.1 Parameter Value Conventions

Parameter values can be a name, a number, or both.

When a range is given for a parameter value, all values in the range are valid except where a step size is specified. Enter all values *without* commas.

When the default value for a parameter displayed as **-1** or **Default**, the actual value is extracted from the underlying routing protocol engine.

4.4.2 About Show Commands

When the output of a show command has more lines than can be displayed on your terminal, you are prompted for a response on how to display the remaining output. For example:

```
#show running-config
enable
vlan-database
vlan 1,10
exit
configure
switch mac-address 00:01:10:00:03:01
switch default-vlan 1
switch aging-time 300
ip address 10.1.1.1 255.255.255.0
vlan 1
name "Default VLAN"
exit
vlan 10
name "VLAN-10"
exit
<?> - help.
```

At the <?> - help prompt, you have the following options:

- Press **?** or enter **help** to view the options.
- Press **q** to exit the show command and display the command prompt.
- Press **p** to display the next page from the show command.
- Press the **spacebar** to display the remaining output from the show command.
- Press the **Enter** key to display the next line from the show command.

4.4.2.1 Show Filtering

ONS Rev. 1.1 adds Show Filtering functionality, extending the show command, allowing you to filter the data displayed on the screen to display only desired information.

The previous implementation of the show command allowed displaying the user information only in the predefined quantities and sequence, and thus made the user look through vast amounts of information in order to find what they need. It required additional time, concentration, and effort. It also imposed certain restrictions on the way the information was presented.

The Show Command Filtering functionality presents new possibilities for users and removes restrictions of the information presentation. This allows extending the existing method of information presentation in the CLI, making it more convenient without altering its structure and implementation.

The command syntax of Show Command Filtering functionality is as follows:

`show ... | include <rx>` – Shows only fields containing a specified word (symbol).
`show ... | exclude <rx>` – Shows fields which do not contain a specified word (symbol).
`show ... | begin <rx> [end <rx>]` – Shows a specified range of fields.
`show ... | grep [-v] <rx>` – Shows fields containing or not containing a specified word (symbol).

Examples of using the Show Comand Filtering Functionality:

```
Switch (config)#show system

Ethernet Switch Type .................... SimSwitch Switch
Name .................................... ONS CoreSwitch
Model ................................... ONS
Platform ................................ SimSwitch
Chip Version ............................ 2.0
Chip Subtype ............................ simswitch
API Version ............................. SimSwitch 2.0.0
Software Version ........................ trunk
CPU ..................................... x86_64
CPU Architecture ........................ x86_64
OS ...................................... Linux
OS Version .............................. 3.5.0-36-generic
Serial Number ........................... N/A
IP Address .............................. 10.1.1.1
Mask .................................... 255.255.255.0
Gateway ................................. N/A
MAC Address ............................. 00:11:22:33:44:55
Default VLAN ............................ 1

Switch (config)#
Switch (config)#show system | begin Platform end CPU

Platform ................................ SimSwitch
Chip Version ............................ 2.0
Chip Subtype ............................ simswitch
API Version ............................. SimSwitch 2.0.0
Software Version ........................ trunk
CPU ..................................... x86_64

Switch (config)#show system | include Platform

Platform ................................ SimSwitch

Switch (config)#show system | include CPU

CPU ..................................... x86_64
CPU Architecture ........................ x86_64

Switch (config)#show system | include .*o|O.*

Name .................................... ONS CoreSwitch
Model ................................... ONS
Platform ................................ SimSwitch
Chip Version ............................ 2.0
API Version ............................. SimSwitch 2.0.0
```

```
Software Version ........................ trunk
OS Version .............................. 3.5.0-36-generic

Switch (config)#show system | include .*o|O.* | include .*i|I.*

Name .................................... ONS CoreSwitch
Platform ................................ SimSwitch
Chip Version ............................ 2.0
API Version ............................. SimSwitch 2.0.0
Software Version ........................ trunk
OS Version .............................. 3.5.0-36-generic

Switch (config)#
```

4.4.3 Comments

There is an option of adding comments after commands in CLI. In order to add a comment, enter "!" symbol after the command syntax. The "!" symbol and the command syntax must be separated with a space. Anything following the "!" symbol will not be recognized by CLI as command syntax.

4.5 Command Shortcuts

The auto-completion function reduces the number of characters you need to enter to access a command, mode, or parameter. To invoke the auto-complete function, enter a few letters at the prompt and use the **Tab** key or the **Spacebar** to auto-complete the command.

If there is more than one item that matches the entry, the corresponding commands and modes are displayed. If there is only one item that matches the entry, use Spacebar to auto-complete it.

For example:

```
#c (followed by the Tab key displays the command and mode options)
clear configure copy cpu
#co (followed by the Tab key displays the command and mode options)
#configure copy
#con (followed by the Tab or the Spacebar key auto-completes the command)
#configure
(config) #switch a (followed by the Tab key or the Spacebar auto-completes the command parameter)
(config) #switch aging-time
```

See also, Getting Context-Sensitive Help.

4.6 Keyboard Shortcuts

Table 4-3 lists the key combinations you can use to edit commands or increase the speed of command entry.

Table 4-3. Command Line Editing Shortcuts

Shortcut	Description
Ctrl+A	Move cursor to the beginning for the line
Ctrl+E	Move cursor to the end of the line
Ctrl+F	Move cursor forward one character
Ctrl+B	Move cursor backward
Esc+F	Moves forward one word
Esc+B	Moves backwards one word

Ctrl+P	Previous command
Ctrl+N	Next command
Ctrl+W	Delete the word to the left from the cursor
Ctrl+U	Delete the whole line
Ctrl+T	Swap or transpose the current character with the one before it
Ctrl+K	Erase characters from the cursor to end of the line
CTRL+X+ Backspace	Erase characters from the cursor to beginning of the line
Esc+D	Delete from Cursor to end of word
Delete	Removes the character to the right of the cursor
Backspace	Removes the character to the left of the cursor
Up Arrow	Allows you to scroll forward through previous commands
Down Arrow	Allows you to scroll backwards through previous commands
Ctrl+L	Clears screen
Ctrl+R	Allows you to search in the command history
Tab	Command autocomplete
Ctrl+C	Exit. Exit from the mode

4.7 The no Command

The **no** keyword is a specific form of an existing command and does not represent a new or distinct command. Almost every configuration command has a **no** form. Use the **no** prefix to reverse the action of a command or reset a parameter value to the default value.

For example, the **no arp** configuration command reverses the ARP function for an interface. Use the command *without* the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default.

To view the available **no** commands for a given mode, use the following command from any configuration mode:

```
(modeName) #no ?
```

4.8 CLI Severity Messages

If you enter a command and the system is unable to execute it, an severity message appears. Table 4-4 describes the most common CLI error messages.

Table 4-4. CLI Error Messages

Message Type	Description
Notice!	These messages are providing some additional, activity-related information.
Alert!	Messages that are notifying user about system-related events.
Warning!	Messages warn that user activated activities might have consequences that you do not anticipate. Warning messages normally provide the opportunity to continue an activity or to cancel it.
Error!	Messages indicate that an error has occurred.
Debug!	This type of messages is used by technical staff for debug purposes.

4.9 Command Modes

CLI commands are grouped into modes and submodes. Each mode and submode provides a functional grouping of commands. When in a given mode or submode, the command prompt includes the identifier for the current mode. The available modes are based on the installed software modules and the user privilege level, see "Access Levels". The command mode hierarchy and the mode access methods are as follows:

Command	Mode and Submode Command	Submode	Mode name
>			User
>enable	#		Privilege
#vlan-database	(vlan)#		VLAN Creation and Deletion
#configure	(config) #		Global Configuration
	(config) #**interface** *interfaceName*	(config-if *interfaceName*) #	Port Interface Configuration
	(config) #**interface** *vlanNumber*	(if-vlan *vlanNumber*) # (route-if *vlanNumber*) #	VLAN Interface Configuration
	(config) #**interface mgmt-ethernet**	(config-if) #	Management Port Interface Configuration
	(config) #**interface port-channel** *portChannelNumber*	(config-if) #	Port Channel Interface Configuration
	(config) #**router ospf**	(config-router) #	OSPF Configuration
	(config) # **spanning-tree mst configuration**	(config-mst) #	Spanning Tree Configuration
	(config) # **vlan** *vlanNumber*	(config-vlan) #	VLAN Simple Configuration
	(config) # **interface tunnel** *tunnelNumber*	(config-if) #	Tunneling Interface Configuration
	(config) # **interface loopback**	(config-if) #	Interface Loopback

See also, "Navigating Command Modes" .

4.10 Navigating Command Modes

To change modes, enter the mode name at the prompt. For example:

```
# configure
```

The mode name then forms part of the prompt. For example:

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

To view the commands and submodes for a given mode, enter the **Tab** key at the mode prompt. For example:

```
(config)#
access-list        arp                auto-shutdown      exit
fan                help               interface          ip
lacp               lldp               logging
mac-address-table  mls                monitor            no
ntp                ovs                password           port-channel
power-supply       radius-server      router             spanning-tree
storm-control      switch             tacacs-server      traceroute
username           vlan
```

To view a description of each command and submode, enter **?** or **help** at the mode prompt. For example:

```
(config)#?
access-list        Add an access list entry.
arp                Set a static ARP entry.
auto-shutdown      Confirure system auto-shutdown parameters.
exit               Exit the mode.
fan                Configure system fans.
help               Show help information.
interface          Configure interfaces.
ip                 Global IP configuration subcommands.
lacp               Configure LACP globally.
lldp               Configure LLDP options.
logging            Configure message logging facilities.
mac-address-table  Configure MAC address table.
mls                Configure Multilayer switching globally.
monitor            Configure system monitoring parameters.
no                 Negate a command or set its defaults.
ntp                Configure Network Time Protocol (NTP).
ovs                Configure Open-vSwitch.
password           Change current user password.
port-channel       Enable global configuration for lacp and lags.
power-supply       System power supply configuration.
radius-server      Manage RADIUS server settings.
router             Enable a routing process.
spanning-tree      Configure spanning tree.
storm-control      Configure storm control.
switch             Configure switch.
tacacs-server      Manage TACACS server settings.
traceroute         Configure traceroute packet processing.
```

```
username             Manage user settings.
vlan                 Configure VLANs
```

To access a submode, enter the submode name at the prompt. The new mode name forms part of the prompt. For example:

```
(config) # interface xe1
(config-if xe1) #
```

To return to the previous mode, use the **exit** command. For example:

```
(config-if xe1)# exit
(config) # exit
#exit
>
```

You are now in the User mode. Enter **exit** to terminate the CLI session.
For a list of command modes, see "Command Modes".

4.11 About the CLI Reference Chapters

The CLI Reference chapters describe the command line interface (CLI) commands for the ONP. The commands allow you to configure ONP and view the current configuration. The commands are classified as follows:

- Platform Commands
- Layer 2 Commands
- Layer 3 Commands

For a list of all commands alphabetically, see `Command Index.`

4.11.1 CLI Command Fields

The CLI command fields and formats are as follows:

command name

This field provides a description of the command.

Command Syntax	Shows how to enter the command at the command prompt.
Command Mode	Shows the command mode name and how to access the command mode.
Syntax Description	Where applicable, provides a description of the command parameters and options.
Command Default	Where applicable, shows the default values for parameters and options.
Examples	Provides example usage of the command.
System Response	Where applicable, provides a description of the output fields.
Revision	Indicates the revision in which the command description was last modified.
Related Commands	Provides a list of other commands of interest.

To help you identify commands that provide access to a command mode, the **(mode)** string forms part of the command name. For example:

configure (mode)
spanning-tree mst configuration (mode)

When the same command name is available in more than one command mode, the mode name forms part of the command name heading. For example:

mls qos map (config-if)
mls qos map (config)

4.12 Saving ONP Configuration Changes

Changes made from the CLI are implemented upon command execution and are stored in volatile memory. To save the changes permanently, you must access the Privilege mode (#) and save the changes to non-volatile memory. For example:

```
#save config
Configuration saving is in progress. It may take few minutes.#
```

See also, Restoring ONP Configuration .

4.13 Restoring ONP Configuration

You can restore the ONP configuration to the previously saved configuration or to the default configuration.

See also, Saving ONP Configuration Changes.

4.13.1 Restoring the Saved Configuration

To delete the unsaved changes made during the current CLI session and restore the ONP configuration to the *saved* configuration, you must access the Privileged mode (#) and restore the configuration. For example:

```
>enable
#restore config
Proceed with restore operation? ('yes'/'no'): yes#
```

4.13.2 Restoring the Default Configuration

To delete the unsaved changes made during the current CLI session and restore the ONP configuration to the *default* configuration, you must access the Privileged mode (#) and clear the configuration. For example:

```
>enable
#clear config
Proceed with clear operation? ('yes'/'no'): yes
Configuration clearing is in progress.#
```

For information on the default configuration, see `Platform Default Configuration`.

4.14 Viewing the Current Configuration

To view the current ONP configuration you can use the **show running-config** command. To view detailed output you can run the following CLI **show** commands:

From the User Mode:

```
>show arp
>show arp static
>show arp configuration
>show cpu
>show cpu all
>show cpu thresholds
>show disk
>show disk thresholds
>show disk performance
>show disk performance thresholds
>show interface
>show interface interfaceName
>show mac-address-table
>show mac-address-table macAddress
>show memory
>show memory thresholds
>show monitor
>show traceroute
>show version
```

```
>show vlan
>show vlan vlanId
```

From the Privileged Mode:

```
#show access-groups
#show access-groups interfaceName
#show access-lists
#show access-lists accessListNumber
#show access-lists actions
#show access-lists actions accessListNumber
#show access-lists expressions
#show access-lists expressions accessListNumber
#show access-lists rules
#show access-lists rules accessListNumber
#show access-lists statistics
#show access-lists statistics accessListNumber
#show arp
#show arp configuration
#show arp static
#show channel-group
#show channel-group portChannel
#show channel-group portChannel admin
#show channel-group portChannel remote
#show channel-group admin
#show channel-group remote
#show clock
#show cpu
#show cpu all
#show cpu thresholds
#show dcb app local
#show dcb app local map
#show dcb app local status
#show dcb app map
#show dcb app remote
#show dcb app remote map
#show dcb app remote status
#show dcb app status
#show dcb cn
#show dcb cn local
#show dcb cn remote
#show dcb dcbx
#show dcb dcbx local
#show dcb dcbx remote
#show dcb ets-conf
#show dcb ets-reco
#show dcb ets-conf local
#show dcb ets-conf remote
#show dcb ets-reco local
#show dcb ets-reco remote
#show dcb pfc
#show dcb pfc local
#show dcb pfc remote
#show disk
#show disk thresholds
#show disk performance
#show disk performance thresholds
```

```
#show dot1q-tunnel customer vlan mapping interfaces interfaceName
#show dot1q-tunnel encapsulation interfaces interfaceName
#show dot1q-tunnel interfaces
#show dot1q-tunnel interfaces interfaceName
#show dot1q-tunnel provider vlan mapping interfaces interfaceName
#show environment all
#show environment auto-shutdown
#show environment auto-temp
#show environment fans
#show environment fans configuration
#show environment fans thresholds
#show environment power-supply
#show environment power-supply status
#show environment power-supply thresholds
#show environment temperature
#show environment temperature thresholds
#show interface
#show interface transceiver
#show interface interfaceName
#show interface interfaceName transceiver
#show interface mgmt-ethernet
#show interface mgmt-ethernet statistics
#show interface mgmt-ethernet thresholds
#show interface port-channel
#show interface port-channel portChannel
#show interface port-channel portChannel admin
#show interface port-channel portChannel detail
#show interface port-channel portChannel remote
#show interface port-channel admin
#show interface port-channel detail
#show interface port-channel neighbor
#show ip bgp
#show ip bgp ipAddress
#show ip bgp ipAddress ipMask
#show ip bgp aggregate-address ipAddress ipMask
#show ip bgp attribute-info
#show ip bgp cidr-only
#show ip bgp community
#show ip bgp community communityNumber
#show ip bgp community local-as
#show ip bgp community no-advertise
#show ip bgp community no-export
#show ip bgp community-info
#show ip bgp community-list listNumber
#show ip bgp community-list listNumber exact match
#show ip bgp community-list listName
#show ip bgp community-list listName exact match
#show ip bgp confederation peers
#show ip bgp confederation peers peerId
#show ip bgp dampened-paths
#show ip bgp distance admin
#show ip bgp distance network
#show ip bgp filter-list listName
#show ip bgp flap-statistics
#show ip bgp flap-statistics ipAddress
#show ip bgp flap-statistics ipAddress ipMask
#show ip bgp flap-statistics cidr-only
```

```
#show ip bgp flap-statistics filter-list listName
#show ip bgp flap-statistics prefix-list listName
#show ip bgp flap-statistics regexp regularExpression
#show ip bgp flap-statistics route-map mapName
#show ip bgp ipv4 multicast
#show ip bgp ipv4 multicast ipAddress
#show ip bgp ipv4 multicast ipAddress ipMask
#show ip bgp ipv4 multicast cidr-only
#show ip bgp ipv4 multicast community
#show ip bgp ipv4 multicast community communityNumber
#show ip bgp ipv4 multicast community local as
#show ip bgp ipv4 multicast community no-advertise
#show ip bgp ipv4 multicast community no-export
#show ip bgp ipv4 multicast community-list listNumber
#show ip bgp ipv4 multicast community-list listNumber exact match
#show ip bgp ipv4 multicast community-list listName
#show ip bgp ipv4 multicast community-list listName exact match
#show ip bgp ipv4 multicast filter-list listName
#show ip bgp ipv4 multicast neighbors
#show ip bgp ipv4 multicast neighbors ipAddress
#show ip bgp ipv4 multicast prefix-list listName
#show ip bgp ipv4 multicast regexp regularExpression
#show ip bgp ipv4 multicast route-map mapName
#show ip bgp ipv4 multicast rsclient ipAddress
#show ip bgp ipv4 multicast rsclient ipAddress ipAddress
#show ip bgp ipv4 multicast rsclient ipAddress ipAddress ipMask
#show ip bgp ipv4 multicast rsclient summary
#show ip bgp ipv4 multicast summary
#show ip bgp ipv4 unicast ipAddress ipMask
#show ip bgp ipv4 unicast cidr-only
#show ip bgp ipv4 unicast community
#show ip bgp ipv4 unicast community communityNumber
#show ip bgp ipv4 unicast community local-as
#show ip bgp ipv4 unicast community no-advertise
#show ip bgp ipv4 unicast community no-export
#show ip bgp ipv4 unicast community-list listNumber
#show ip bgp ipv4 unicast community-list listNumber exact match
#show ip bgp ipv4 unicast community-list listName
#show ip bgp ipv4 unicast community-list listName exact match
#show ip bgp ipv4 unicast filter-list listName
#show ip bgp ipv4 unicast neighbors
#show ip bgp ipv4 unicast neighbors ipAddress
#show ip bgp ipv4 unicast paths
#show ip bgp ipv4 unicast regexp regularExpression
#show ip bgp ipv4 unicast route-map mapName
#show ip bgp ipv4 unicast rsclient ipAddress
#show ip bgp ipv4 unicast rsclient ipAddress ipAddress
#show ip bgp ipv4 unicast rsclient ipAddress ipAddress ipMask
#show ip bgp ipv4 unicast rsclient summary
#show ip bgp ipv4 unicast summary
#show ip bgp neighbor
#show ip bgp neighbor ipAddress
#show ip bgp neighbor connection
#show ip bgp neighbor connection ipAddress
#show ip bgp neighbor remote-as
#show ip bgp neighbor remote-as ipAddress
#show ip bgp neighbors
```

```
#show ip bgp neighbors ipAddress
#show ip bgp network
#show ip bgp network ipAddress ipMask
#show ip bgp paths
#show ip bgp peer-group
#show ip bgp peer-group peerGroup
#show ip bgp peer-group members
#show ip bgp peer-group members peerGroup
#show ip bgp prefix-list listName
#show ip bgp regexp regularExpression
#show ip bgp route-map mapName
#show ip bgp route-redistribute
#show ip bgp router
#show ip bgp rsclient ipAddress
#show ip bgp rsclient ipAddress ipAddress
#show ip bgp rsclient ipAddress ipAddress ipMask
#show ip bgp rsclient summary
#show ip bgp scan detail
#show ip bgp status
#show ip bgp view viewName
#show ip bgp view viewName ipAddress
#show ip bgp view viewName ipAddress ipMask
#show ip bgp view viewName ipv4 multicast rsclient summary
#show ip bgp view viewName ipv4 multicast summary
#show ip bgp view viewName ipv4 unicast rsclient summary
#show ip bgp view viewName ipv4 unicast summary
#show ip bgp view viewName neighbors
#show ip bgp view viewName neighbors ipAddress
#show ip bgp view viewName neighbors ipAddress advertised-routes
#show ip bgp view viewName neighbors ipAddress received-routes
#show ip bgp view viewName rsclient ipAddress
#show ip bgp view viewName rsclient ipAddress ipAddress
#show ip bgp view viewName rsclient ipAddress ipAddress ipMask
#show ip bgp view viewName rsclient summary
#show ip bgp view viewName summary
#show ip igmp
#show ip ospf
#show ip ospf area
#show ip ospf area filtering
#show ip ospf area network-map
#show ip ospf area route-redistribute
#show ip ospf area virtual-link
#show ip ospf area summary
#show ip ospf config
#show ip ospf database
#show ip ospf database asbr-summary
#show ip ospf database external
#show ip ospf database network
#show ip ospf database router
#show ip ospf database summary
#show ip ospf interface routeInterface keys
#show ip ospf neighbor
#show ip ospf neighbor detail
#show ip ospf route
#show ip route
#show ip route static
#show lldp
```

```
#show lldp interface
#show lldp interface interfaceName
#show lldp neighbors
#show lldp neighbors interface interfaceName
#show lldp traffic
#show lldp traffic interface interfaceName
#show lldp interface
#show lldp interface interfaceName
#show lldp neighbors interface interfaceName
#show logging
#show logging last linesNumber
#show logging logfile
#show logging logfile end-time endTime
#show logging logfile start-time startTime end-time endTime
#show mac-address-table
#show mac-address-table macAddress
#show memory
#show memory thresholds
#show mls qos bandwidth
#show mls qos bandwidth interfaceName
#show mls qos map dot1p-cos
#show mls qos map dscp-cos
#show mls qos scheduling
#show mls qos scheduling interfaceName
#show monitor
#show ip name-server
#show ntp-associations
#show ovs
#show ovs bridges
#show ovs flows
#show ovs ports
#show ovs resources
#show port-channel
#show interface
#show interface interfaceName transceiver
#show interface mgmt-ethernet
#show interface mgmt-ethernet statistics
#show interface mgmt-ethernet thresholds
#show interface port-channel
#show interface port-channel portChannel
#show interface port-channel portChannel admin
#show interface port-channel portChannel detail
#show interface port-channel portChannel remote
#show interface port-channel admin
#show interface port-channel detail
#show interface port-channel neighbor
#show interface transceiver
#show interface vlan
#show interface vlan vlanNumber
#show radius-server
#show radius-server hostname hostName
#show radius-server ip-address ipAddress
#show running-config
#show running-config interface interfaceRange
#show running-config interface mgmt-ethernet
#show running-config interface port-channel portChannelRange
#show saved-configs
```

```
#show snmp
#show snmp community
#show snmp engine-id
#show snmp group
#show snmp host
#show snmp user
#show snmp view
#show software-upgrade state
#show spanning-tree
#show spanning-tree interface
#show spanning-tree interface interfaceName
#show spanning-tree interface port-channel portChannel#show spanning-tree mst
mstRegion
#show spanning-tree mst configuration
#show spanning-tree mst interface
#show spanning-tree mst interface interfaceName
#show spanning-tree mst interface port-channel portChannel#show statistics
#show statistics interface interfaceName
#show storm-control
#show system
#show tacacs-server
#show tacacs-server hostname hostName
#show tacacs-server ip-address ipAddress
#show tech-support
#show traceroute
#show users
#show username
#show username userName
#show version
#show vlan
#show vlan vlanNumber
```

Note: To display output from multiple show commands, you can copy a set of show commands to the clipboard and paste the commands at the CLI prompt. For example:

```
show arp
show channel-group local
show channel-group remote
show interface
show tacacs-server
```

4.15 Platform Default Configuration

The platform default configuration is as follows:

4.16 System Logs

The ONP logs are stored in volatile memory at **/var/log**. The logs are captured nightly and stored in non-volatile memory in **/var/preserve**. The logs are also captured upon a controlled halt.

Note: The **/var/log** directory is stored in volatile memory and is cleared upon platform restart. Example logs are as follows:

To obtain a permanent record of the system logs, you can redirect the logs to an external storage device. For more information, see the *ONP XML-RPC Reference and User Guide*.

4.17 Core Files

When processes terminate unexpectedly, a core file is generated in the **/tmp** directory. The core file name format is **core**.*executable-name*.**pid**. Core files are kept for seven days, afterwhich they are deleted. The directory and files are stored in volatile memory and are cleared upon platform restart.

5. Platform Commands

This section covers the platform-specific commands for the Privileged mode and Global Configuration mode.

5.1 User Execution Mode Commands

show cpu

Shows CPU utilization, load averages and thresholds, as well as displays data per CPU/core.

Command Syntax	**show cpu [all | thresholds]**	
Command Modes	User Execution Mode	>
Syntax Description	**all**	Show data related to all CPU instances.
	thresholds	Show CPU subsystem threshold configuration.
Command Default	This command has no default settings.	

Examples

```
#show cpu
#show cpu all
#show cpu thresholds
```

System Response

The output fields for **cpu** and **cpu all** are as follows:

Field	Description
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Time	
Value	

The output fields for **cpu threshold** are as follows:

Field	Description
Enabled	Controls the enabling/disabling of the threshold. If set false (default) the threshold is not enabled, if set true the threshold is enabled.
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Failure max	The upper bound of acceptable values for the failure threshold. If unset, the upper bound of the failure threshold is disabled (i.e. defaults to negative infinity).
Failure min	Sets the lower bound of acceptable values for the failure threshold. If unset, the lower bound of the failure threshold is disabled (i.e. defaults to negative infinity
Warning max	The upper bound of acceptable values for the warning threshold. If unset, the upper bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Warning min	The lower bound of acceptable values for the warning threshold. If unset, the lower bound of the warning threshold is disabled (i.e. defaults to negative infinity).

Hits	Delay creating the notification until the threshold has been passed *hits* number of times. When a notification has been generated, or when a subsequent value is inside the threshold, the counter is reset.

Revision 1.0.1

Related Commands

`cpu threshold`

show memory

Displays memory utilization and thresholds.

Command Syntax **show memory [thresholds]**

Command Modes User Execution Mode >

Syntax Description

thresholds	Shows memory subsystem threshold configuration.

Command Default This command has no default settings.

Examples

```
#show memory
#show memory threshold
```

System Response The output fields for **memory** are as follows:

Field	Description
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Time	
Value	

The output fields for **memory threshold** are as follows:

Field	Description
Enabled	Controls the enabling/disabling of the threshold. If set false (default) the threshold is not enabled, if set true the threshold is enabled.
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Failure max	The upper bound of acceptable values for the failure threshold. If unset, the upper bound of the failure threshold is disabled (i.e. defaults to negative infinity).
Failure min	Sets the lower bound of acceptable values for the failure threshold. If unset, the lower bound of the failure threshold is disabled (i.e. defaults to negative infinity
Warning max	The upper bound of acceptable values for the warning threshold. If unset, the upper bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Warning min	The lower bound of acceptable values for the warning threshold. If unset, the lower bound of the warning threshold is disabled (i.e. defaults to negative infinity).

Hits	Delay creating the notification until the threshold has been passed *hits* number of times. When a notification has been generated, or when a subsequent value is inside the threshold, the counter is reset.

Revision 1.0.1

Related Commands

`memory threshold`

show disk

Displays disk utilization data and thresholds.

Command Syntax **show disk [thresholds]**

Command Modes User Execution Mode >

Syntax Description		
	thresholds	Shows disk subsystem threshold configuration.

Command Default This command has no default settings.

Examples

```
#show disk
#show disk threshold
```

System Response The output fields for **disk** are as follows:

Field	Description
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Time	
Value	

The output fields for **disk threshold** are as follows:

Field	Description
Enabled	Controls the enabling/disabling of the threshold. If set false (default) the threshold is not enabled, if set true the threshold is enabled.
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Failure max	The upper bound of acceptable values for the failure threshold. If unset, the upper bound of the failure threshold is disabled (i.e. defaults to negative infinity).
Failure min	Sets the lower bound of acceptable values for the failure threshold. If unset, the lower bound of the failure threshold is disabled (i.e. defaults to negative infinity
Warning max	The upper bound of acceptable values for the warning threshold. If unset, the upper bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Warning min	The lower bound of acceptable values for the warning threshold. If unset, the lower bound of the warning threshold is disabled (i.e. defaults to negative infinity).

	Hits	Delay creating the notification until the threshold has been passed *hits* number of times. When a notification has been generated, or when a subsequent value is inside the threshold, the counter is reset.
Revision	1.0.1	
Related Commands	`disk threshold`	

show disk performance

Shows disk performance related data.

Command Syntax **show disk performance[thresholds]**

Command Modes User Execution Mode >

Syntax Description **thresholds** Shows disk subsystem threshold configuration.

Command Default This command has no default settings.

Examples

```
#show disk
#show disk performance
#show disk performance threshold
```

System Response The output fields for **disk performance** are as follows:

Field	Description
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Time	
Value	

The output fields for **disk performance threshold** are as follows:

Field	Description
Enabled	Controls the enabling/disabling of the threshold. If set false (default) the threshold is not enabled, if set true the threshold is enabled.
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Failure max	The upper bound of acceptable values for the failure threshold. If unset, the upper bound of the failure threshold is disabled (i.e. defaults to negative infinity).
Failure min	Sets the lower bound of acceptable values for the failure threshold. If unset, the lower bound of the failure threshold is disabled (i.e. defaults to negative infinity
Warning max	The upper bound of acceptable values for the warning threshold. If unset, the upper bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Warning min	The lower bound of acceptable values for the warning threshold. If unset, the lower bound of the warning

	threshold is disabled (i.e. defaults to negative infinity).
Hits	Delay creating the notification until the threshold has been passed *hits* number of times. When a notification has been generated, or when a subsequent value is inside the threshold, the counter is reset.

Revision 1.0.1

Related Commands

`disk performance threshold`

5.2 Privileged Mode Commands

clear config

Resets the ONP configuration to the default configuration values and clears the ONP statistics.
To view a summary of the current platform configuration before applying the **clear config** command, use the **show running-config** command. To view the detailed configuration of the platform, use the **show** commands as described in Viewing the Current Configuration.

Command Syntax	**clear config**	
Command Modes	Privileged Mode	#
Syntax Description	This command does not have any parameters or key words.	
Command Default	None.	

Examples

```
#clear config
Clearing configuration ...
```

Revision 1.0.1

Related Commands

```
show running-config
clear statistics
restore config
save config
reload
```

clear statistics

Resets the ONP statistics for all ports or the specified port.

Command Syntax	**clear statistics interface** [<*interfaceName*>]	
Command Modes	Privileged Mode	#
Syntax Description	**interface**	Clears statistics data on an interface.
	interfaceName	Name of an interface port. For example, **xe1**.
Command Default	None.	

Examples

```
#show statistics interface xe1
#clear statistics interface xe1
Proceed with clear operation? ('yes'/'no'):yes
#show statistics interface xe1
#clear statistics
```

```
Proceed with clear operation? ('yes'/'no'):yes
```

System Response

The cleared statistics for the interface ports are as follows:

Field	Description
Rx Broadcast Pkts	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. (RFC 1573)
Rx Discards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to higher-layer protocol. (RFC 1213)
Rx Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher layer protocol. (RFC 1213)
Rx Multicast Pkts	The number of packets, delivered by this sub-layer to a higher (sub-) layer, which were addressed to a multicast address at this sub-layer. (RFC 1573)
Rx NUcast Pkts	The number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher layer protocol. (RFC 1213)
Rx Octecs	The total number of octets received on the interface, including framing characters. (RFC 1213)
Rx Ucast Pkt	The number of subnetwork-unicast packets delivered to a higher-layer protocol. (RFC 1213)
Tx Broadcast Pkts	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. (RFC 1573)
Tx Discards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. (RFC 1213)
Tx Errors	The number of outbound packets that could not be transmitted because of errors. (RFC 1213)
Tx Multicast Pkts	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. (RFC 1573)
Tx NUcast Pkts	The total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent. (RFC 1213)
Tx Octets	The total number of octets transmitted out of the interface, including framing characters. (RFC 1213)
Tx QLen	The length of the output packet queue (in packets). (RFC 1213)
Tx Ucast Pkts	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent. (RFC 1213)

Revision 1.2

Related Commands

```
clear config
show interface
show statistics
```

copy

Copies a file to or from the local system. File names may contain a user and host specification to indicate that the file is to be copied to/from that host. Local file names can be made explicit using absolute or relative pathnames to avoid scp treating file names containing ':' as host specifiers.

Command Syntax **copy <**_source_**> <**_destination_**>**

Command Modes Privileged Mode #

Syntax Description

source	Specifies the source from which file will be copied.
destination	Specifies the destination to which file will be copied.

Command Default This command has no default values.

Examples

```
#copy flash:.bashrc scp://username1@147.11.118.99/tmp
```

Revision 1.0.1

Related Commands

`delete`
`dir`

cpu threshold

Configures CPU subsystem thresholds.
Type is an option parameter. If specified, it will control which threshold is being configured, either warning or failure. If not specified, the configured threshold defaults to warning.

Command Syntax

cpu threshold metric {idle | interrupt | nice | softirq | steal | system | user | wait | short-term-load-avg | mid-term-load-avg | long-term-load-avg} { {hits <_hits_**>} | {type { { warning { {low <**_low_**> [high <**_high_**>]} | {high <**_high_**> [low <**_low_**>]} } } | { failure { {low <**_low_**> [high <**_high_**>]} | {high <**_high_**> [low <**_low_**>]} } } } } }**

no cpu threshold metric {idle | interrupt | nice | softirq | steal | system | user | wait | short-term-load-avg | mid-term-load-avg | long-term-load-avg} [hits | {type { {warning [{low [high]} | {high [low]}]} | {failure [{low [high]} | {high [low]}]} }}]

Command Modes Privileged Mode #

Syntax Description

metric	Specifies for which indicator threshold is being configured.
idle	Specifies the percentage of time that the CPU or CPUs were idle and the system did not have an outstanding disk I/O request.
interrupt	Specifies the percentage of time spent by the CPU or CPUs to service hardware interrupts.

nice	Specifies the percentage of CPU utilization that occurred while executing at the user level with nice priority.
softirq	Specifies the percentage of time spent by the CPU or CPUs to service software interrupts.
steal	Specifies the percentage of time spent in involuntary wait by the virtual CPU or CPUs while the hypervisor was servicing another virtual processor.
system	Specifies the percentage of CPU utilization that occurred while executing at the system level (kernel). Note that this does not include time spent servicing hardware and software interrupts.
user	The percentage of CPU utilization that occurred while executing at the user level (application).
wait	Specifies the percentage of time that the CPU or CPUs were idle during which the system had an outstanding disk I/O request.
short-term-load-avg	Specifies the 1-minute CPU load average.
mid-term-load-avg	Specifies the 10-minute CPU load average.
long-term-load-avg	Specifies the 15-minute CPU load average.
low	Configures the lower bound of acceptable values for the warning or failure threshold.
low	Lower bound of acceptable values.
high	Configures the upper bound of acceptable values for the warning or failure threshold.
high	Upper bound of acceptable values.
hits	Delays generating a WARNING or FAILURE log until the threshold has been crossed 'hits' number of times.
hits	Delay of creating the notification until the threshold has benn passed.
type	Specifies which threshold is being configured, either warning or failure. If not specified, the configured threshold defaults to warning.
warning	Configures warning threshold.
failure	Configures failure threshold.

Command Default

Examples

```
#cpu threshold metric steal low 10 type failure
#cpu threshold metric idle hits 10
#cpu threshold metric idle high 5 type warning
#no cpu threshold metric idle hits type warning
```

Revision 1.2

Related Commands

`show cpu`

delete file

Deletes a file from the local system.

Command Syntax **delete file <*fileName*>**

Command Modes Privileged Mode #

Syntax Description

file	Deletes a file from the local file system.
fileName	Identifies the file to be deleted.

Command Default This command has no default values.

Examples

```
#delete file username_image
```

Revision 1.2

Related Commands

`copy`
`dir`

dir

Displays a list of files on a file system.

Command Syntax **dir**

Command Modes Privileged Mode #

Syntax Description This command does not have any parameters or key words.

Command Default This command has no default values.

Examples

```
#dir
```

System Response The output contains the list of the files on a file systems and contains the following fileds:

Field	Description
File Name	Name of the file.
Size	Size of the file.

Revision 1.0.1

Related Commands

`copy`
`delete`

disk performance threshold

Configures disk performance thresholds.

Command Syntax

disk performance threshold metric {read-bytes|write-bytes|read-time|write-time|read-operations|write-operations|read-ops-merged|write-ops-merged} { {hits <*hits* >} | {type { { warning { {low <*low*> [high <*high*>]} | {high <*high*> [low <*low*>]} } } | { failure { {low <*low*> [high <*high*>]} | {high <*high*> [low <*low*>]} } } } } }

no disk performance threshold metric {read-bytes|write-bytes|read-time|write-time|read-operations|write-operations|read-ops-merged|write-ops-merged} [hits | type { {warning [{low [high]} | {high [low]}]} | {failure [{low [high]} | {high [low]}]} }]

Command Modes

Privileged Mode	#

Syntax Description

metric	Specifies for which indicator threshold is being configured.
read-bytes	The number of bytes read from disk.
write-bytes	The number of bytes written to disk.
read-time	The average disk read time.
write-time	The average disk write time.
read-operations	The number of disk read operations issued.
write-operations	The number of disk write operations issued.
read-ops-merged	The number of disk read operations that were merged into other, already queued, operations.
write-ops-merged	The number of disk write operations that were merged into other, already queued, operations.
low	Configures the lower bound of acceptable values for the warning or failure threshold.
low	Lower bound of acceptable values.
high	Configures the upper bound of acceptable values for the warning or failure threshold
high	Upper bound of acceptable values.
hits	Delays generating a WARNING or FAILURE log until the threshold has been crossed 'hits' number of times.
hits	Delay of creating the notification until the threshold has benn passed.
type	Specifies which threshold is being configured, either warning or failure. If not specified, the configured threshold defaults to warning.
warning	Configures warning threshold
failure	Configures failure threshold.

Command Default

The ARP list has no entries.

Examples

```
#disk performance threshold metric write-ops-merged high 100
#disk performance threshold metric read-bytes low 1000 type
```

```
warning
#disk performance threshold metric read-time hits 1000
#no disk performance threshold metric read-bytes high type
failure
```

Revision 1.2

Related Commands

`show disk performance`

disk threshold

Configures disk subsystem thresholds.
Type is an option parameter. If specified, it will control which threshold is being configured, either warning or failure. If not specified, the configured threshold defaults to warning.

Command Syntax

disk threshold [instance {onsp|root}] metric {free|used|reserved} { {hits <*hits* >} | {type { { warning { {low <*low*> [high <*high*>]} | {high <*high*> [low <*low*>]} } } | { failure { {low <*low*> [high <*high*>]} | {high <*high*> [low <*low*>]} } } } } }

no disk threshold [instance {onsp|root}] metric {free|used|reserved} [hits | type { {warning [{low [high]} | {high [low]}]} | {failure [{low [high]} | {high [low]}]} }]

Command Modes Privileged Mode #

Syntax Description

instance	Configures threshold instance.
onsp	Configures threshold for the onsp instance.
root	Configures threshold for the root instance.
metric	Specifies for which indicator threshold is being configured.
free	Specifies the amount of free disk space available per device or mounted filesystem.
used	Specifies the amount of used disk space per device or mounted filesystem.
reserved	Specifies the amount of reserved disk space per device or mounted filesystem.
low	Configures the lower bound of acceptable values for the warning or failure threshold.
low	Lower bound of acceptable values.
high	Configures the upper bound of acceptable values for the warning or failure threshold.
high	Upper bound of acceptable values.
hits	Delays generating a WARNING or FAILURE log until the threshold has been crossed 'hits' number of times.
hits	Delay of creating the notification until the threshold has benn passed.

type	Specifies which threshold is being configured, either warning or failure. If not specified, the configured threshold defaults to warning.
warning	Configures warning threshold.
failure	Configures failure threshold.

Command Default

Examples

```
#disk threshold metric reserved high 10
#disk threshold metric free
#disk threshold metric reserved hits 10 type failure
#disk threshold instance root metric free low 1 high 100
type warning
#no disk threshold instance onsp metric free high type
failure
```

Revision 1.2

Related Commands

`show disk`

exit

Accesses the previous command mode or quits the current CLI session. For a list of command modes, see Command Modes.

Command Syntax **exit**

Command Modes All Modes

Revision 1.0.1

Examples

```
(config-if xe1) #exit (Returns to the global configuration
mode.)
(config) #exit (Returns to the Privileged mode.)
#exit (Returns to the User mode.)
>exit (Quits the current CLI session.)
```

memory threshold

Configures collecting and monitoring platform metrics and indirectly platform faults for memory subsystem. **Type** is an option parameter. If specified, it will control which threshold is being configured, either warning or failure. If not specified, the configured threshold defaults to warning.

Command Syntax

memory threshold metric {buffered | cached | free | used} { {hits <*hits*>} | {type { { warning { {low <*low*> [high <*high*>]} | {high <*high*> [low <*low*>]} } } | { failure { {low <*low*> [high <*high*>]} | {high <*high*> [low <*low*>]} } } } }

no memory threshold metric {buffered | cached | free | used} [hits |

type { {warning [{low [high]} | {high [low]}]} | {failure [{low [high]} | {high [low]}]} }]

Command Modes	Privileged Mode	#

Syntax Description

metric	Specifies for which indicator threshold is being configured.
buffered	Specifies the amount of physical RAM used for file buffers.
cached	Specifies the amount of physical RAM used as cache memory.
free	Specifies the amount of physical RAM left unused by the system.
used	Specifies the total usable RAM left free, buffered and cached RAM.
low	Configures the lower bound of acceptable values for the warning or failure threshold.
low	Lower bound of acceptable values.
high	Configures the upper bound of acceptable values for the warning or failure threshold.
high	Upper bound of acceptable values.
hits	Delays generating a WARNING or FAILURE log until the threshold has been crossed 'hits' number of times.
hits	Delay of creating the notification until the threshold has benn passed.
type	Specifies which threshold is being configured, either warning or failure. If not specified, the configured threshold defaults to warning.
warning	Configures warning threshold.
failure	Configures failure threshold.

Command Default

Examples

```
#memory threshold metric buffered high 10
#memory threshold metric cached hits 10
#memory threshold metric used low 10 type warning
#no memory threshold metric buffered high type failure
```

Revision 1.2

Related Commands

`show memory`

reload

Reloads the operating system into the switch. All CLI sessions are terminated and all communication with the platform ports is terminated. All unsaved configuration changes are lost.

Command Syntax **reload**

Command Modes Privileged Mode #

Examples

```
#reload
Proceed with reload? (‘yes/’no’): yes
The system is going down for reboot NOW!
```

Revision 1.0.1

Related Commands

`clear config`
`clear statistics`
`restore config`
`save config`

restore config

Deletes the unsaved changes made during the current CLI session and restores the ONP configuration to the *saved* configuration.

Command Syntax **restore config [<*fileName*>]**

Syntax Description	*fileName*	Name of the configuration to be restored
Command Modes	Privileged Mode	#

Examples

```
#restore config
Restoring configuration ...

#restore config necconfig12
Restoring configuration ...

#
```

Revision 1.2

Related Commands

`clear config`
`clear statistics`
`reload`
`save config`

save config

Saves the configuration changes to non-volatile memory. The configuration is retained as the working configuration for the ONP. If the parameter value is specified, the configuration is saved to a file that can be exported and imported later.

Command Syntax **save config [<*fileName*>]**

Syntax Description	*fileName*	Name of the configuration to be saved.
Command Modes	Privileged Mode	#

Examples

```
#save config
Configuration saving is in progress. It may take few
minutes.
#save config necconfig12
Configuration saving is in progress. It may take few
minutes.

Switch #dir

File name Size
--------- ----

Switch #software config-data export necconfig12 neccnofig2

Configuration export is in progress. This may take few
minutes.

Configuration data has been exported to the file
'necconfig2'.

Switch #dir

File name Size
-------------- -------
necconfig2 1216379

Switch #software config-data import necconfig2

Notice! Configuration from the file 'necconfig2' has been
successfully imported.

Switch #
```

Revision 1.2

Related Commands

`restore config`
`clear config`

show applications

Shows data on configured applications.

Command Syntax **show applications <*applicationName*>**

Command Modes Privileged Mode #

Syntax Description

applications	Shows application data.
applicationName	Application name to show configuration for.

Command Default This command has no default settings.

Examples

```
#show applications

Application ............................
ONSNorthboundServer
Version ................................ 1.00
Type ................................... MgmtSrv
Administrative State ................... Run
Operational State ...................... Run
Log Level .............................. Notice

Application ............................ ONSSnmpServer
Version ................................ 1.00
Type ................................... Control
Administrative State ................... Run
Operational State ...................... Run
Log Level .............................. Notice

Application ............................
ONSApplicationServer
Version ................................ 1.00
Type ................................... AppSrv
Administrative State ................... Run
Operational State ...................... Run
Log Level .............................. Notice

#show applications ONSSnmpServer

Application ............................ ONSSnmpServer
Version ................................ 1.00
Type ................................... Control
Administrative State ................... Run
Operational State ...................... Run
Log Level .............................. Notice
```

System Response

The output fields for **show applications** are as follows:

Field	Description
Application	Application name.
Version	Application version.
Type	Application type.
Administrative State	Application admin state.
Operational State	Application operational status.
Log Level	Application syslog message reporting minmal level.

The output fields for **show applications ONSSnmpServer** are as follows:

Field	Description
Application	Application name.
Version	Application version.
Type	Application type.
Administrative State	Application admin state.
Operational State	Application operational status.
Log Level	Application syslog message reporting minmal level.

Revision	1.2
Related Commands	`logging application level`

show cpu

Shows cpu utilization, load averages and thresholds, as well as displays data per CPU/core.

Command Syntax **show cpu [all | thresholds]**

Command Modes	Privileged Mode	#
Syntax Description	**all**	Show data related to all CPU instances.
	thresholds	Show CPU subsystem threshold configuration.

Command Default This command has no default settings.

Examples

```
#show cpu
#show cpu all
#show cpu thresholds
```

System Response The output fields for **cpu** and **cpu all** are as follows:

Field	Description
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Time	
Value	

The output fields for **cpu threshold** are as follows:

Field	Description
Enabled	Controls the enabling/disabling of the threshold. If set false (default) the threshold is not enabled, if set true the threshold is enabled.
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Failure max	The upper bound of acceptable values for the failure threshold. If unset, the upper bound of the failure threshold is disabled (i.e. defaults to negative infinity).
Failure min	Sets the lower bound of acceptable values for the failure threshold. If unset, the lower bound of the failure threshold is disabled (i.e. defaults to negative infinity
Warning max	The upper bound of acceptable values for the warning threshold. If unset, the upper bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Warning min	The lower bound of acceptable values for the warning threshold. If unset, the lower bound of the warning threshold is disabled (i.e. defaults to negative infinity).

	Hits	Delay creating the notification until the threshold has been passed *hits* number of times. When a notification has been generated, or when a subsequent value is inside the threshold, the counter is reset.
Revision	1.0.1	

Related Commands

`cpu threshold`

show disk

Display disk utilization data and thresholds.

Command Syntax **show disk [thresholds]**

Command Modes	Privileged Mode	#
Syntax Description	**thresholds**	Shows disk subsystem threshold configuration.

Command Default This command has no default settings.

Examples

```
#show disk
#show disk threshold
```

System Response The output fields for **disk** are as follows:

Field	Description
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Time	
Value	

The output fields for **disk threshold** are as follows:

Field	Description
Enabled	Controls the enabling/disabling of the threshold. If set false (default) the threshold is not enabled, if set true the threshold is enabled.
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Failure max	The upper bound of acceptable values for the failure threshold. If unset, the upper bound of the failure threshold is disabled (i.e. defaults to negative infinity).
Failure min	Sets the lower bound of acceptable values for the failure threshold. If unset, the lower bound of the failure threshold is disabled (i.e. defaults to negative infinity
Warning max	The upper bound of acceptable values for the warning threshold. If unset, the upper bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Warning min	The lower bound of acceptable values for the warning threshold. If unset, the lower bound of the warning

		threshold is disabled (i.e. defaults to negative infinity).
	Hits	Delay creating the notification until the threshold has been passed *hits* number of times. When a notification has been generated, or when a subsequent value is inside the threshold, the counter is reset.

Revision 1.0.1

Related Commands

`disk threshold`

show disk performance

Shows disk performance related data.

Command Syntax **show disk performance[thresholds]**

Command Modes Privileged Mode #

Syntax Description **thresholds** Shows disk subsystem threshold configuration.

Command Default This command has no default settings.

Examples

```
#show disk
#show disk performance
#show disk performance threshold
```

System Response The output fields for **disk performance** are as follows:

Field	Description
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Time	
Value	

The output fields for **disk performance threshold** are as follows:

Field	Description
Enabled	Controls the enabling/disabling of the threshold. If set false (default) the threshold is not enabled, if set true the threshold is enabled.
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Failure max	The upper bound of acceptable values for the failure threshold. If unset, the upper bound of the failure threshold is disabled (i.e. defaults to negative infinity).
Failure min	Sets the lower bound of acceptable values for the failure threshold. If unset, the lower bound of the failure threshold is disabled (i.e. defaults to negative infinity
Warning max	The upper bound of acceptable values for the warning threshold. If unset, the upper bound of the warning threshold is disabled (i.e. defaults to negative infinity).

Warning min	The lower bound of acceptable values for the warning threshold. If unset, the lower bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Hits	Delay creating the notification until the threshold has been passed *hits* number of times. When a notification has been generated, or when a subsequent value is inside the threshold, the counter is reset.

Revision 1.0.1

Related Commands

`disk performance threshold`

show environment

Displays hardware environment information.

Command Syntax **show environment all|{fans [configuration]|[thresholds]} |{power-supply[status]|[thresholds]}|{temperature [thresholds]}| auto-temp | auto-shutdown**

Command Modes Privileged Mode #

Syntax Description

all	Displays a detailed listing of all environmental monitor parameters.
fans	Displays fans information.
configuration	Displays the current environment monitoring configuration for fans.
thresholds	Displays fans thresholds configuration.
power-supply	Displays information on power supply status.
status	Displays power supply status.
thresholds	Displays power-supply thresholds configuration.
temperature	Displays temperature information.
thresholds	Displays temperature thresholds configuration.
auto-temp	Displays automatic temperature – fan speed dependency.
auto-shutdown	Displays auto shutdown configuration information.

Command Default This command has no default settings.

Examples

```
#show environment all
#show environment auto-temp
#show environment temperature thresholds
#show environment fans configuration
```

System Response The output fields for **environment auto-shutdown** are as follows:

Field	Description
Index	

State	Current auto-shutdown state.
Temperature	Auto-shutdown threshold temperature.

The output fields for **environment auto-temp** are as follows:

Field	Description
Index	
Temperature	Temperature at which to adjust fan speed, in degress Celsius.
Speed	Fan speed, in percentage.

The output fields for **environment fans** are as follows:

Field	Description
ID	Logical fan identification number.
State	Administrative state of the fan.
Mode	Administrative mode of the fan.
Speed	Administrative speed (in percentage), only used if administrative mode is set to ‘manual’.

The output fields for **environment fans configuration** are as follows:

Field	Description
ID	Logical fan identification number.
Type	Type of fan.
State	Operational state of the fan.
Mode	Operational mode of the fan.
Speed	Operational speed.

The output fields for **environment fans thresholds** are as follows:

Field	Description
Enabled	Controls the enabling/disabling of the threshold. If set false (default) the threshold is not enabled, if set true the threshold is enabled.
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Failure max	The upper bound of acceptable values for the failure threshold. If unset, the upper bound of the failure threshold is disabled (i.e. defaults to negative infinity).
Failure min	Sets the lower bound of acceptable values for the failure threshold. If unset, the lower bound of the failure threshold is disabled (i.e. defaults to negative infinity
Warning max	The upper bound of acceptable values for the warning threshold. If unset, the upper bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Warning min	The lower bound of acceptable values for the warning threshold. If unset, the lower bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Hits	Delay creating the notification until the threshold has been passed *hits* number of times. When a notification has been generated, or when a subsequent value is inside the threshold, the counter is reset.

The output fields for **environment power-supply** are as follows:

Field	Description

Power Supply	Logical power supply ID.
Administrative State	Current administrative state.
Operational State	Current operational state.
Operational Status	Current health status.

The output fields for **environment power-supply status** are as follows:

Field	Description
Controller	Logical power supply controller ID.
Controller Name	Supply voltage description.
Admin Output Voltage Mode	
Admin Output Voltage	Administrative output voltage (millivolts).
Operational Output Voltage Mode	
Operational Output Voltage	Operational output voltage (millivolts).
Operational Output Current	Operational output current (milliamps).
Operational Input 12V	12V supply voltage (millivolts).
Operational Input 3.3V	3.3V supply voltage (millivolts).
Operational Input Current	12V input current consumption (milliamps).
Operational Fault Code	Fault code bitmap.

The output fields for **environment power-supply thresholds** are as follows:

Field	Description
Enabled	Controls the enabling/disabling of the threshold. If set false (default) the threshold is not enabled, if set true the threshold is enabled.
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Failure max	The upper bound of acceptable values for the failure threshold. If unset, the upper bound of the failure threshold is disabled (i.e. defaults to negative infinity).
Failure min	Sets the lower bound of acceptable values for the failure threshold. If unset, the lower bound of the failure threshold is disabled (i.e. defaults to negative infinity
Warning max	The upper bound of acceptable values for the warning threshold. If unset, the upper bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Warning min	The lower bound of acceptable values for the warning threshold. If unset, the lower bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Hits	Delay creating the notification until the threshold has been passed *hits* number of times. When a notification has been generated, or when a subsequent value is inside the threshold, the counter is reset.

The output fields for **environment temperature** are as follows:

Field	Description
ID	Sensor ID.
Type	Type of sensor.
Temperature	Sensor value.

The output fields for **environment temperature thresholds** are as follows:

Field	Description
Enabled	Controls the enabling/disabling of the threshold. If set false (default) the threshold is not enabled, if set true the threshold is enabled.
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Failure max	The upper bound of acceptable values for the failure threshold. If unset, the upper bound of the failure threshold is disabled (i.e. defaults to negative infinity).
Failure min	Sets the lower bound of acceptable values for the failure threshold. If unset, the lower bound of the failure threshold is disabled (i.e. defaults to negative infinity
Warning max	The upper bound of acceptable values for the warning threshold. If unset, the upper bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Warning min	The lower bound of acceptable values for the warning threshold. If unset, the lower bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Hits	Delay creating the notification until the threshold has been passed *hits* number of times. When a notification has been generated, or when a subsequent value is inside the threshold, the counter is reset.

Revision 1.0.1

Related Commands

`fan`
`power-supply`
`auto-shutdown`
`monitor-environment`

show interface mgmt-ethernet

Displays the information of the Ethernet management port.

Command Syntax **show interface mgmt-ethernet [thresholds|statistics]**

Command Modes Privileged Mode #

Syntax Description

thresholds	Shows KPI threshold configuration for interface subsystem.
statistics	Shows KPI last read data for interface subsystem.

Command Default This command has no default settings.

Examples

```
#show interface mgmt-ethernet
#show interface mgmt-thresholds
#show interface mgmt-statistics
```

System Response The output fields for **interface mgmt-ethernet** are as follows:

Field	Description
Port	Name of the management port.
Hostname	Host name for the management port.
IP Address Mode	Link configuration mode for the management port
IP Address	IP address for the management port.
IP Mask	IP mask for the management port.
Gateway	Gateway IP address for the management port.
Administrative State	Administrative state for the management port.
MTU	Maximum frame size for the management port.
Speed	Port speed in Mbps.
Duplex	Link duplex mode for the management port
Autonegotiation	Link autonegotiation mode for the management port.

The output for **interface mgmt-ethernet statistics** is the following:

Field	Description
Subsystem	Name of the interface subsystem.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Time	
Value	

The output fields for **interface mgmt-ethernet thresholds** are as follows:

Field	Description
Enabled	
Subsystem	Name of the interface subsystem.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Failure max	Upper bound of acceptable values for the failure threshold.
Failure min	Lower bound of acceptable values for the failure threshold.
Warning max	Upper bound of acceptable values for the warning threshold.
Warning min	Lower bound of acceptable values for the warning threshold.
Hits	The number of times a WARNING or FAILURE log generation is delayed until the threshold has been crossed.

Revision 1.2

Related Commands

`ip address`
`gateway`
`shutdown`
`ip address`
`speed`
`autoneg`
`duplex`
`max-frame-size`
`hostname`
`threshold metric`

show logging

Displays the running syslog configuration.

Command Syntax

show logging [last *<linesNumber>***|{logfile [start-time** *<startTime>* **[end-time** *<endTime>***]]|[end-time** *<endTime>***]}]**

Command Modes

Privileged Mode #

Syntax Description

last	Displays the last number of lines in the logging file.
<linesNumber>	Specifies the number of lines to display. The range is 1-9999.
logfile	Displays the messages in the log file that have a time stamp within the span entered. If you do not enter an end time, the current time is used.
start-time	Specifies start-point time.
end-time	Specifies end-point time.
startTime	Start-point time. Time should be entered in the format YYYY MM DD HH:MM:SS.
endTime	End-point time. Time should be entered in the format YYYY MM DD HH:MM:SS.

Command Default

This command has no default settings.

Examples

```
#show logging
#show logging last 10
#show logging logfile end-time 2012 12 12 12:12:12
```

System Response

The output fields for **logging** are as follows:

Field	Description
IP Address	IP address of the syslog server.
Protocol	The protocol configured to send syslog messages to the syslog server.
Local Port	Port from with logs should be sent.
Remote Port	Port on the remote logserver to send logs.
Severity	Severity level of syslog message.
Facility	Syslog server logging facility.

Revision

1.0.1

Related Commands

`logging host transport`
`logging host syslog`

show memory

Displays memory utilization and thresholds.

Command Syntax

show memory [thresholds]

Command Modes Privileged Mode #

Syntax Description **thresholds** Shows memory subsystem threshold configuration.

Command Default This command has no default settings.

Examples

```
#show memory
#show memory threshold
```

System Response The output fields for **memory** are as follows:

Field	Description
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Time	
Value	

The output fields for **memory threshold** are as follows:

Field	Description
Enabled	Controls the enabling/disabling of the threshold. If set false (default) the threshold is not enabled, if set true the threshold is enabled.
Subsystem	Subsystem to which this indicator belongs.
Instance	Instance of the subsystem to which this indicator belongs.
Indicator	Indicator to monitor.
Failure max	The upper bound of acceptable values for the failure threshold. If unset, the upper bound of the failure threshold is disabled (i.e. defaults to negative infinity).
Failure min	Sets the lower bound of acceptable values for the failure threshold. If unset, the lower bound of the failure threshold is disabled (i.e. defaults to negative infinity
Warning max	The upper bound of acceptable values for the warning threshold. If unset, the upper bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Warning min	The lower bound of acceptable values for the warning threshold. If unset, the lower bound of the warning threshold is disabled (i.e. defaults to negative infinity).
Hits	Delay creating the notification until the threshold has been passed *hits* number of times. When a notification has been generated, or when a subsequent value is inside the threshold, the counter is reset.

Revision 1.0.1

Related Commands

`memory threshold`

show ntp-associations

Shows the set of NTP (Network Time Protocol) connections configured.

Command Syntax **show ntp-associations**

Command Modes	Privileged Mode	#

Syntax Description This command does not have any parameters or keywords.

Command Default This command has no default settings.

Examples

```
#show ntp-associations
```

System Response The output fields for **ntp-assosiations** are as follows:

Field	Description
Address	IP address of the server to synchronize with.
NTP version	NTP version number to be used to communicate with the server.
IBurst	Specifies that when the server is reachable, a burst of packets should be sent rather than just one.
Burst	Specifies that when the server is reachable, a burst of packets should be sent rather than just one.
Prefer	Specifies if the server is marked as preferred.

Revision 1.0.1

Related Commands

`ntp server`
`ntp peer`

show radius-server

Shows information about registered radius-servers.

Command Syntax **show radius-server [hostname <*hostName*>] | [ip-address <*ipAddres*>]**

Command Modes	Privileged Mode	#

Syntax Description

hostname	Shows radius-server with specified hostname.
hostname	Host name of the server.
ip-address	Shows radius-server with specified IP address.
ipAddress	IP address of the server.

Command Default This command has no default settings.

Examples

```
#show radius-server
#show radius-server hostname www.hostname.com
#show radius-server ip-address 1.1.1.1
```

System Response The output fields for **radius-server** are as follows:

Field	Description
Host	The host name or ip address of the server

Timeout	Number of seconds a router waits for a reply to a RADIUS request before retransmitting the request.

Revision 1.0.1

Related Commands

radius-server host

show saved-configs

Shows saved system configurations.

Command Syntax **show saved-configs**

Command Modes Privileged Mode #

Syntax Description This command does not have any parameters or keywords.

Command Default This command has no default settings.

Examples

```
#show saved-configs
```

System Response The output fields for **saved-configs** are as follows:

Field	Description
Version	Version of the previously saved configuration file.
Directory	Location of the previously saved configuration file.

Revision 1.0.1

Related Commands

show snmp

Shows the status of Simple Network Management Protocol (SNMP) communications.

Command Syntax **show snmp**

Command Modes Privileged Mode #

Syntax Description This command does not have any parameters or keywords.

Command Default This command has no default settings.

Examples

```
#show snmp
```

System Response The output fields for **snmp** are as follows:

Field	Description
Chassis	Administratively-assigned name for the device.
Contact	System contact.
Description	System description.
Location	System location.

Revision 1.0.1

Related Commands

```
snmp-server chassis-id
snmp-server location
snmp-server description
snmp-server contact
```

show snmp group

Shows the names of groups on the router and the security model and the status of the different views.

Command Syntax **show snmp group**

Command Modes Privileged Mode #

Syntax Description **group** Shows the names of groups on the router and the security model and the status of the different views.

Command Default This command has no default settings.

Examples

```
#show snmp group
```

System Response The output fields for **snmp group** are as follows:

Field	Description
Group Name	Name of the group.
Security Model	Security model applied to the group (v1, v2c, v3).
Security Level	Security level applied to the group (auth, noauth, priv).
Read View	View to which the group has read-only privileges.
Write View	View to which the group has read/write privileges.
Notify View	View to which the group has the ability to raise traps and informs.

Revision 1.0.1

Related Commands

```
snmp-server group
```

show snmp user

Displays information on each SNMP username configured on the system.

Command Syntax **show snmp user**

Command Modes Privileged Mode #

Syntax Description This command does not have any parameters or keywords.

Command Default This command has no default settings.

Examples

```
#show snmp user
```

System Response The output fields for **snmp user** are as follows:

Field	Description
User name	Name of the user.
Authentication level	HMAC-MD5-96 or HMAC-SHA-96 authentication level.
Encryption algorithm	CBC-DES or AES encryption.
Permissions	
Security model	Security model applied to the named user.
Group name	Name of the group with which the user is associated.
View	View(s) to which the named user is restricted, separated by commas.

Revision 1.0.1

Related Commands

`snmp-server group`

show snmp host

Displays the remote receiver of an SNMP notification operation.

Command Syntax **show snmp host**

Command Modes Privileged Mode #

Syntax Description This command does not have any parameters or keywords.

Command Default This command has no default settings.

Examples

```
#show snmp host
```

System Response The output fields for **snmp host** are as follows:

Field	Description
Host address	Name or address of the receiver.
OID	OIDs (Object Identifiers) that will be forwarded to the named host.
Transport	L4 protocol via which the receiver is connected.
Port	L4 port.

Revision 1.0.1

Related Commands

`snmp-server host`

show snmp community

Displays the community access string to permit access to the SNMP.

Command Syntax **show snmp community**

Command Modes Privileged Mode #

Syntax Description This command does not have any parameters or keywords.

Command Default This command has no default settings.

Examples

```
#show snmp community
```

System Response The output fields for **snmp community** are as follows:

Field	Description
Community name	Name of the community string.
View name	Name of the view for which the community string applies
Storage type	Type of the access.
IP Address	Address(es) allowed to use the community string to gain access to the SNMP agent. Separate addresses should be followed by IP Mask (after a "/") and separated by commas.

Revision 1.0.1

Related Commands

`snmp-server community`

show snmp view

Displays information of each named view configured on the system.

Command Syntax **show snmp view**

Command Modes Privileged Mode #

Syntax Description This command does not have any parameters or keywords.

Command Default This command has no default settings.

Examples

```
#show snmp view
```

System Response The output fields for **snmp view** are as follows:

Field	Description
View name	Name of the view.
OID	OID tree (subtree) to which the view refers.

View type	Type of the view.

Revision 1.0.1

Related Commands

`snmp-server view`

show software-upgrade state

Shows current status of the software upgrade procedure.

Command Syntax **show software-upgrade state**

Command Modes Privileged Mode #

Syntax Description This command does not have any parameters or keywords.

Command Default This command has no default settings.

Examples

```
#show software-upgrade state
```

System Response The output fields for **software-upgrade state** are as follows:

Field	Description
State	State of software upgrade process.
Detailed Info	Detailed information on the software upgrade process.
Image Name	Name of the image from which the software upgrade started.
Target Bank	Target bank.

Revision 1.0.1

Related Commands

show tacacs-server

Shows information about registered TACACS servers.

Command Syntax

show tacacs-server

show tacacs-server hosname <*hostname*>

show tacacs-server ip-address <*ipAddress*>

Command Modes Privileged Mode #

Syntax Description

hostname	Shows TACACS server with specified hostname.
hostName	The Fully Qualified Domain Name of the TACACS server.

	ip-address	Shows TACACS server with specified Ip-address.
	ipAddress	Ipv4 address of the TACACS server.

Command Default This command has no default settings.

Examples

```
#show tacacs-server
#show tacacs-server hostname www.hostname.com
#show tacacs-server ip-address 1.1.1.1
```

System Response The output fields for **tacacs-server** are as follows:

Field	Description
Host	Name or IP address of the host.
Timeout	Global timeout value set with the tacacs-server timeout command for this server only.

Revision 1.0.1

Related Commands

show usersname

Shows information about registered users.

Command Syntax **show usersname [<*userName*>]**

Command Modes Privileged Mode #

Syntax Description *userName* Displays the information for the specified user.

Command Default This command has no default settings.

Examples

```
#show usersname
#show usersname name.surname
```

System Response The output fields for **username** are as follows:

Field	Description
Name	Name of the user
Privilege	Privilege level of the user, that is specific access and ability permissions assigned to the user. The CLI has three privilege levels (cli, priv, and admin).
Shell	The login shell for the user.
Authentication	Specifies the types of authentication available to this user.

Revision 1.0.1

Related Commands

`username authentication`

snmp-server chassis-id

Configures an administratively-assigned name for this managed node.

Command Syntax	**snmp-server chassis-id <***chassisId***>**	
Command Modes	Privileged Mode	#
Syntax Description	*chassisId*	Name for this managed device.
Command Default	This command does not have any default values.	
Examples	`#snmp-server chassis-id DEVICE`	
Revision	1.0.1	

Related Commands	`show snmp`
	`snmp-server location`
	`snmp-server contact`
	`snmp-server description`	

snmp-server community

Configures the community access string to permit access to the SNMP.

Command Syntax	**snmp-server community <***community***> [view <***viewName***>] [{ro|rw} [<***addressRange***>]]**	
Command Modes	Privileged Mode	#
Syntax Description	*community*	Name of the community.
	viewName	Name of the view for which the community string applies.
	ro	Allows the named community only read access.
	rw	Allows the named community full read-write access.
	addressRange	Source address allowed to use the community string to gain access to the SNMP agent. Source source can either be a specific hostname (or address), or a subnet - represented as IP/MASK (e.g. 10.10.10.0/255.255.255.0), or IP/BITS (e.g. 10.10.10.0/24), or the IPv6 equivalents.
Command Default	This command does not have any default values.	

Examples

```
#snmp-server community COMM view VIEW
#snmp-server community COMM view VIEW ro
#snmp-server community COMM view VIEW ro
```

```
1.1.1.0/255.255.255.0,2.2.2.0/24,3.3.3.3
#snmp-server community COMM view VIEW rw
#snmp-server community COMM view VIEW rw
1.1.1.0/255.255.255.0,2.2.2.0/24,3.3.3.3
#snmp-server community COMM
#snmp-server community COMM ro
#snmp-server community COMM ro
1.1.1.0/255.255.255.0,2.2.2.0/24,3.3.3.3
#snmp-server community COMM rw
#snmp-server community COMM rw
1.1.1.0/255.255.255.0,2.2.2.0/24,3.3.3.3
```

Revision 1.2

Related Commands

`show snmp community`

snmp-server contact

Configures the system contact string.

Command Syntax **snmp-server contact <***contact***>**

Command Modes Privileged Mode #

Syntax Description *contact* System contact string.

Command Default This command does not have any default values.

Examples

```
#snmp-server contact CONTACT
```

Revision 1.0.1

Related Commands

`show snmp`
`snmp-server chassis-id`
`snmp-server location`
`snmp-server description`

snmp-server description

Configures the system description string.

Command Syntax **snmp-server description <***description***>**

Command Modes Privileged Mode #

Syntax Description *description* System description string.

Command Default This command does not have any default values.

Examples

```
#snmp-server description DESC
```

Revision 1.0.1

Related Commands

`show snmp`
`snmp-server chassis-id`
`snmp-server contact`
`snmp-server location`

snmp-server group

Configures a new SNMP group, or configures a table that maps SNMP users to SNMP views.

Command Syntax **snmp-server group [<*groupName*> {v1 | v2c | {v3 {auth | noauth | priv}}}] {read | write | notify} <*view*>**

Command Modes Privileged Mode #

Syntax Description

groupName	Name of the group being created and/or edited.
v1	Sets the security model version to 1.
v2c	Sets the security model version to 2c.
v3	Sets the security model version to 3.
auth	Sets security level to 'auth'.
noauth	Sets security level to 'noauth'.
priv	Sets security level to 'priv'.
read	Allows read only access to the specified SNMP group.
write	Allows read-write access to the specified SNMP group.
notify	Grants only notify privileges for the specified SNMP group.
view	View to which the group has appropriate privileges.

Command Default This command does not have any default values.

Examples

```
#snmp-server group GR1 v1 notify NOTVIEW
#snmp-server group GR2 v2c read READVIEW
#snmp-server group GR3 v3 priv write WRTVIEW
```

Revision 1.2

Related Commands

`show snmp group`

snmp-server host

Configures the remote receiver of an SNMP notification operation. The **no** form of the command removes the remote receiver of an SNMP notification operation.

Command Syntax

snmp-server host <*hostName*> **[tcp6-port** <*tcp6Port*>**|udp6-port** <*udp6Port*>**|tcp-port** <*tcpPort* >**|udp-port** <*udpPort* >**|ssh-port** <*sshPort*>**|dtls-port** <*dtlsPort*>**|unix-socket]** <*OID*>

no snmp-server host <*hostName*> **{all |** <*OID*>**}**

snmp-server host <*hostName*> **{trap | inform} { {{v1 | v2c}** <*communityString*>**} | {v3** <*userName*> **{noauth | {auth {md5 |sha}** <*authPassword*> **} | {priv {md5 |sha}** <*authPassword*> **{des | aes}** <*privPassword*>**}}} } [udp-port** <*port*>**]**

no snmp-server host <*hostName*> **[trap | inform]**

Command Modes	Privileged Mode	#

Syntax Description

hostName	Name or address of the receiver.
tcp6Port	Configures TCP over IPv6 port on remote host to send to.
udp6Port	Configures UDP over IPv6 port on remote host to send to.
tcpPort	Configures TCP port on remote host to send to.
udpPort	Configures UDP port on remote host to send to.
sshPort	Configures SSH port on remote host to send to.
dtlsPort	Configures DTLS port on remote host to send to.
unix-socket	Configure unix socket to send to.
OID	Sets OIDs (Object Identifiers) that will be forwarded to the named host.
all	Removes all existing receivers with specified name or address.
trap	Sends SNMP traps to this host.
inform	Sends SNMP informs to this host.
v1	Sets the security model version to 1.
v2c	Sets the security model version to 2c.
communityString	Community string for SNMPv1/v2c transactions.
v3	Sets the security model version to 3.
userName	User name used for authenticated SNMPv3 messages.
noauth	Sets security level to 'noauth'.
auth	Sets security level to 'auth'.

md5	Specifies HMAC-MD5-96 authentication level.
sha	Specifies Secure Hash Algorithm (SHA) authentication level.
authPassword	Sets string that enables the agent to send packets from the host. String length must be at least 8 characters.
priv	Sets security level to 'priv'.
des	Sets the 56-bit Digital Encryption Standard (DES) algorithm for encryption.
aes	Sets the Advanced Encryption Standard (AES) algorithm for encryption.
privPassword	String that specifies the privacy user password. String length must be at least 8 characters.
udp-port	Configures UDP port on remote host to send to.
port	User Datagram Protocol (UDP) port of the host to use.

Command Default

This command does not have any default values.

Examples

```
#snmp-server host 128.224.187.99
#snmp-server host 128.224.187.99 1
#snmp-server host 128.224.187.99 tcp6-port 1
#snmp-server host 128.224.187.99 udp6-port 1
#snmp-server host 128.224.187.99 tcp-port 1
#snmp-server host 128.224.187.99 udp-port 1
#snmp-server host 128.224.187.99 ssh-port 1
#snmp-server host 128.224.187.99 dtls-port 1
#snmp-server host 128.224.187.99 unix-socket
#no snmp-server host 128.224.187.99 all
#no snmp-server host 128.224.187.99 1
#snmp-server host 128.224.187.99 trap v1 <community string>
#snmp-server host 128.224.187.99 inform v3 username noauth
#snmp-server host 128.224.187.99 inform v3 username auth md5
<auth password>
#snmp-server host 128.224.187.99 inform v3 username priv md5
privpassword des <auth password>
#no snmp-server host 128.224.187.99
#no snmp-server host 128.224.187.99 trap
#no snmp-server host 128.224.187.99 inform
```

Revision

1.2

Related Commands

`show snmp host`

snmp-server location

Configures the system location string.

Command Syntax

snmp-server location <*location***>**

Command Modes

Privileged Mode	#

Syntax Description		
	location	Location of the system.

Command Default This command does not have any default values.

Examples

```
#snmp-server location LOC1
```

Revision 1.0.1

Related Commands

`show snmp`
`snmp-server chassis-id`
`snmp-server contact`
`snmp-server description`

snmp-server user

Configures a new user to an SNMP group. The **no** form of the command removes the SNMP user.

Command Syntax

snmp-server user <*userName***> <***groupName***> {tsm | ksm | usm} [auth md5|sha <***authPassword***> priv des|aes <***privPassword***>] [read | write] [<***viewRange***>]**

no snmp-server user <*userName***>**

Command Modes Privileged Mode #

Syntax Description		
	userName	Name of the user being created.
	groupName	Name of the group with which the user is associated.
	tsm	Specifies that SNMP security model with SSH or DTLS support should be used.
	ksm	Specifies that SNMP Kerberos security model should be used.
	usm	Specifies that the SNMPv3 security model should be used.
	md5|sha	Use HMAC-MD5-96 or HMAC-SHA-96 authentication level.
	authPassword	Authentication password.
	des|aes	Use the CBC-DES or AES encryption.
	privPassword	String used to seed encryption of messages to the agent.
	read	Allows read only access to the specified SNMP user.
	write	Allows read-write access to the specified SNMP user.
	viewRange	Named view(s) to which the named user is restricted separated by commas.

Command Default This command does not have any default values.

Examples

```
#snmp-server user USER1 GR1 tsm auth md5 PASSWORD priv des
PASSWORD2 READVIEW,WRTVIEW
#snmp-server user USER2 GR1 tsm auth sha PASSWORD priv aes
```

```
PASSWORD3
#snmp-server user USER1 GR1 ksm auth md5 PASSWORD priv des
PASSWORD2 READVIEW,WRTVIEW
#snmp-server user USER2 GR1 ksm auth sha PASSWORD priv aes
PASSWORD3
#snmp-server user USER1 GR1 usm auth md5 PASSWORD priv des
PASSWORD2 READVIEW,WRTVIEW
#snmp-server user USER2 GR1 usm auth sha PASSWORD priv aes
PASSWORD3
#no snmp-server user USER2
```

Revision 1.2

Related Commands `show snmp user`

snmp-server view

Creates a named view corresponding to a subset of the overall OID tree. Several view entries can be created with the same view name to build up a complex collection of OIDs. The **no** form of the command removes the SNMP view.

Command Syntax

snmp-server view <*viewName*> <*OID*> included|excluded

no snmp-server view <*viewName*> {all | <*OID*>}

Command Modes Privileged Mode #

Syntax Description

viewName	Name of the view being created/edited.
OID	OID tree (subtree) to which the view refers.
all	Removes all SNMP views with specified name.
included|excluded	Specified OID may be included (default) or excluded from the view.

Command Default This command does not have any default values.

Examples

```
#snmp-server view NEWVIEW 1.12.23.12.123.23.2 included
#snmp-server view NEWVIEW 1.12.23.12.123.23.2 excluded
#no snmp-server view NEWVIEW all
#no snmp-server view NEWVIEW 1.12.23.12.123.23.2
```

Revision 1.2

Related Commands `show snmp view`

software config-data

Exports and imports configuration data.

Command Syntax **software config-data {{export <*savedConfigName*>} | import} [<*fileName*>]**

Command Modes Privileged Mode #

Syntax Description

export	Exports the configuration data to a file.

	savedConfigName	Saved configuration name to export.
	import	Imports configuration data from the specified file and applies the imported configuration to the system.
	fileName	Name of the file.

Command Default This command has no default values.

Examples

```
#software config-data import image.tar
#software config-data export image.tar
```

Revision 1.2

Related Commands

software upgrade start

Starts a software upgrade to the image in the indicated file name.

Command Syntax **software upgrade start <*fileName*>**

Command Modes Privileged Mode #

Syntax Description *fileName* Name of the file.

Command Default This command has no default values.

Examples

```
#software upgrade start image.tar
```

Revision 1.0.1

Related Commands

`software upgrade cancel`
`software upgrade load`
`software upgrade commit`

software upgrade load

Loads and starts an installed software image.

Command Syntax **software upgrade load**

Command Modes Privileged Mode #

Syntax Description This command does not have any parameters or key words.

Command Default This command has no default values.

Examples `#software upgrade load`

Revision 1.0.1

Related Commands

`software upgrade cancel`
`software upgrade start`
`software upgrade commit`

software upgrade cancel

Reverts a software upgrade in progress and removes the installed image. If the system has already loaded the new software image, the system reboots back to the old image.

Command Syntax **software upgrade cancel**

Command Modes Privileged Mode #

Syntax Description This command does not have any parameters or key words.

Command Default This command has no default values.

Examples `#software upgrade cancel`

Revision 1.0.1

Related Commands

`software upgrade load`
`software upgrade start`
`software upgrade commit`

software upgrade commit

Make the current software upgrade permanent and complete the upgrade.

Command Syntax **software upgrade commit**

Command Modes Privileged Mode #

Syntax Description This command does not have any parameters or key words.

Command Default This command has no default values.

Examples `#software upgrade commit`

Revision 1.0.1

Related Commands `software upgrade load`
`software upgrade start`

```
software upgrade cancel
```

5.3 Global Configuration Mode Commands

interface mgmt-ethernet

Allows entering the interface mode to configure the management port.

Command Syntax **interface mgmt-ethernet**

Command Modes Configuration Mode `#configure`

Syntax Description This command does not have any parameters or key words.

Command Default This command has no default values.

Examples

```
(config) #interface mgmt-ethernet
(config-if)#
```

Revision 1.0.1

Related Commands

`show interface mgmt-ethernet`

logging application level

Configures application log level.

Command Syntax **[no] logging application <*applicationName*> level {stop | emergency | alert | critical | error | warning | notice | informational | debug}**

Command Modes Global Configuration Mode `(config)#`

Syntax Description

logging	Configures message logging facilities
application	Configures application.
applicationName	Application name. Execute **show application** command in Privileged mode to see the list of configured applications.
level	Sets application log level.
stop	Disables write logging messages by specified application.
emergency	Sets application logging level as emergency.
alert	Sets application logging level as alert.
critical	Sets application logging level as critical.
error	Sets application logging level as error.
warning	Sets application logging level as warning.

notice	Sets application logging level as notice.
informational	Sets application logging level as informational.
debug	Sets application logging level as debug.

Command Default

Examples

```
(config)#logging application onsps level stop
(config)#logging application onsps level emergency
(config)#logging application onsps level alert
(config)#logging application onsps level critical
(config)#logging application onsps level error
(config)#logging application onsps level warning
(config)#logging application onsps level notice
(config)#logging application onsps level informational
(config)#logging application onsps level debug
(config)#no logging application onsps level
```

Revision 1.2

Related Commands `show applications`

logging host transport

Configures syslog server IP address and parameters.

Command Syntax **[no] logging host <*ipAddress*> transport {tcp | udp | tcp6 | udp6} [local-port <*localPort*>] [remote-port <*remotePort*>] [{trap <*severityLevel*>} | emergency | alert | critical | error | warning | notice | informational | debug] [facility <*facilityLevel*>]**

Command Modes Configuration Mode

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

Syntax Description

ipAddress	IP address of the syslog server.
tcp	Configures TCP to send syslog messages to the syslog server.
udp	Configures UDP to send syslog messages to the syslog server.
localPort	Sets the port from with logs should be sent. The range is 1-65535.
remotePort	Sets the port on the remote logserver to send logs. The range is 1-65535.
trap	Configures syslog server logging level (0-7).
emergency	Specifies to send emergency messages (0).
alert	Specifies to send alert messages (1).
critical	Specifies to send critical messages (2).
error	Specifies to send error messages (3).

warning	Specifies to send warning messages (4).
notice	Specifies to send notice messages (5).
informational	Specifies to send informational messages (6).
debug	Specifies to send debug messages (7).
facility	Configures syslog server logging facility (the range is from 0 to 23).

Command Default This command has no default values.

Examples

```
(config)#logging host 1.1.1.1 transport udp
(config)#logging host 1.1.1.1 transport udp6
(config)#logging host 1.1.1.1 transport tcp6
(config)#logging host 1.1.1.1 transport tcp
(config)#logging host 1.1.1.1 transport tcp facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap 1 facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap emergency
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap emergency facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap error
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap error facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap alert
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap alert facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap critical
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap critical facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap warning
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap warning facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap notice
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap notice facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap informational
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap informational facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap debug
(config)#logging host 1.1.1.1 transport tcp local-port 1
trap debug facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
```

```
remote-port 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap 1 facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap emergency
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap emergency facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap error
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap error facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap alert
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap alert facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap critical
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap critical facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap warning
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap warning facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap notice
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap notice facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap informational
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap informational facility 1
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap debug
(config)#logging host 1.1.1.1 transport tcp local-port 1
remote-port 1 trap debug facility 1
(config)#logging host 1.1.1.1 transport tcp remote-port 1
(config)#logging host 1.1.1.1 transport tcp remote-port 1
facility 1
(config)#logging host 1.1.1.1 transport tcp remote-port 1
trap 1
(config)#logging host 1.1.1.1 transport tcp remote-port 1
trap 1 facility 1
(config)#logging host 1.1.1.1 transport tcp remote-port 1
trap debug
(config)#logging host 1.1.1.1 transport tcp remote-port 1
trap debug facility 1
(config)#logging host 1.1.1.1 transport tcp trap 1
(config)#logging host 1.1.1.1 transport tcp trap 1 facility
1
(config)#logging host 1.1.1.1 transport tcp trap debug
(config)#logging host 1.1.1.1 transport tcp trap debug
facility 1
(config)#logging host 1.1.1.1 transport tcp trap emergency
```

```
(config)#logging host 1.1.1.1 transport tcp trap emergency
facility 1
(config)#logging host 1.1.1.1 transport tcp trap alert
(config)#logging host 1.1.1.1 transport tcp trap alert
facility 1
(config)#logging host 1.1.1.1 transport tcp trap critical
(config)#logging host 1.1.1.1 transport tcp trap critical
facility 1
(config)#logging host 1.1.1.1 transport tcp trap error
(config)#logging host 1.1.1.1 transport tcp trap error
facility 1
(config)#logging host 1.1.1.1 transport tcp trap warning
(config)#logging host 1.1.1.1 transport tcp trap warning
facility 1
(config)#logging host 1.1.1.1 transport tcp trap notice
(config)#logging host 1.1.1.1 transport tcp trap notice
facility 1
(config)#logging host 1.1.1.1 transport tcp trap
informational
(config)#logging host 1.1.1.1 transport tcp trap
informational facility 1
(config)#no logging host 1.1.1.1 transport tcp
(config)#no logging host 1.1.1.1 transport tcp6
(config)#no logging host 1.1.1.1 transport udp
(config)#no logging host 1.1.1.1 transport udp6
(config)#no logging host 1.1.1.1 transport udp6 facility
(config)#no logging host 1.1.1.1 transport udp6 trap
(config)#no logging host 1.1.1.1 transport udp6 trap
facility
```

Revision 1.2

Related Commands

`show logging`

logging host syslog

Configures IEFT-syslog protocol to send syslog messages to the syslog server.

Command Syntax **[no] logging host <*ipAddress*> syslog [transport {tcp | udp | tcp6 | udp6} [local-port <*localPort*>] [remote-port <*remotePort*>]] [{trap <*severityLevel*>} | emergency | alert | critical | error | warning | notice | informational | debug] [facility <*facilityLevel*>]**

Command Modes Configuration Mode

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

Syntax Description

ipAddress	IP address of the syslog server.
transport	Sets transport protocol type.
tcp	Sets TCP as a transport for IETF-syslog protocol.
udp	Sets UDP as a transport for IETF-syslog protocol.

udp6	Configures UDP over IPv6 to send syslog messages to the syslog server.
local-port	Configures local port to send syslog messages to the syslog server.
localPort	Local port number from with logs should be sent. The range is 1-65535.
remote-port	Configures remote port to which syslog messages should be sent.
remotePort	Remote port on the remote logserver to send logs to. The range is 1-65535.
trap	Configures syslog server logging level (0-7).
severityLevel	Sends messages with specified severity level.
emergency	Specifies to send emergency messages.
alert	Specifies to send alert messages.
critical	Specifies to send critical messages.
error	Specifies to send error messages.
warning	Specifies to send warning messages.
notice	Specifies to send notice messages.
informational	Specifies to send informational messages.
debug	Specifies to send debug messages.
facility	Configures syslog server logging facility (the range is from 0 to 23).
facilityLevel	Sends messages with specified facility.

Command Default This command has no default values.

Examples

```
(config)#logging host 1.1.1.1 syslog
(config)#logging host 1.1.1.1 syslog facility 1
(config)#logging host 1.1.1.1 syslog trap 1
(config)#logging host 1.1.1.1 syslog trap 1 facility 1
(config)#logging host 1.1.1.1 syslog trap emergency
(config)#logging host 1.1.1.1 syslog trap emergency facility
1
(config)#logging host 1.1.1.1 syslog trap alert
(config)#logging host 1.1.1.1 syslog trap alert facility 1
(config)#logging host 1.1.1.1 syslog trap critical
(config)#logging host 1.1.1.1 syslog trap critical facility
1
(config)#logging host 1.1.1.1 syslog trap error
(config)#logging host 1.1.1.1 syslog trap error facility 1
(config)#logging host 1.1.1.1 syslog trap warning
(config)#logging host 1.1.1.1 syslog trap warning facility 1
(config)#logging host 1.1.1.1 syslog trap notice
(config)#logging host 1.1.1.1 syslog trap notice facility 1
(config)#logging host 1.1.1.1 syslog trap informational
(config)#logging host 1.1.1.1 syslog trap informational
facility 1
```

```
(config)#logging host 1.1.1.1 syslog trap debug
(config)#logging host 1.1.1.1 syslog trap debug facility 1
 (config)#logging host 1.1.1.1 syslog transport tcp
(config)#logging host 1.1.1.1 syslog transport udp
(config)#logging host 1.1.1.1 syslog transport tcp6
(config)#logging host 1.1.1.1 syslog transport udp6
(config)#logging host 1.1.1.1 syslog transport udp6 facility
1
(config)#logging host 1.1.1.1 syslog transport udp6 local-
port 1
(config)#logging host 1.1.1.1 syslog transport udp6 local-
port 1 remote-port 1
(config)#logging host 1.1.1.1 syslog transport udp6 local-
port 1 remote-port 1 trap 1
(config)#logging host 1.1.1.1 syslog transport udp6 local-
port 1 remote-port 1 trap emergency
(config)#logging host 1.1.1.1 syslog transport udp6 local-
port 1 remote-port 1 trap alert
(config)#logging host 1.1.1.1 syslog transport udp6 local-
port 1 remote-port 1 trap critical
(config)#logging host 1.1.1.1 syslog transport udp6 local-
port 1 remote-port 1 trap error
(config)#logging host 1.1.1.1 syslog transport udp6 local-
port 1 remote-port 1 trap warning
(config)#logging host 1.1.1.1 syslog transport udp6 local-
port 1 remote-port 1 trap notice
(config)#logging host 1.1.1.1 syslog transport udp6 local-
port 1 remote-port 1 trap informational
(config)#logging host 1.1.1.1 syslog transport udp6 local-
port 1 remote-port 1 trap debug
(config)#logging host 1.1.1.1 syslog transport udp6 local-
port 1 remote-port 1 debug facility 1

(config)#no logging host 1.1.1.1 syslog
(config)#no logging host 1.1.1.1 syslog facility
(config)#no logging host 1.1.1.1 syslog trap
(config)#no logging host 1.1.1.1 syslog trap facility
```

Revision 1.2

Related Commands

`show logging`

ntp peer

Designates the time-serving hosts to use in case of Network Timing Protocol (NTP) server failure.

Command Syntax **ntp peer <*ipAddress*>|<*name*> [version <*version*>] [key <*key*>] [prefer]**
no ntp {<*ipAddress*> | <*hostname*>}

Command Modes Configuration Mode `(config)#`

Syntax Description

ipAddress	IP address of the server to synchronize with.
name	Hostname of the server to synchronize with.

version	NTP version number to be used to communicate with the server. The range is 1 to 4.
key	Key used to encrypt NTP packets. The range is 1 to 65534.
prefer	Marks the peer as preferred.
ipAddress	NTP IP address to stop synchronizing with.
hostname	NTP hostname stop synchronizing with.

Command Default This command has no default values.

Examples

```
(config) #ntp peer PEER1 version 1 key 1
(config) #ntp peer 10.1.1.100 version 1 key 1
(config) #no ntp PEER1
(config) #no ntp 10.1.1.100
```

Revision 1.2

Related Commands

`show ntp-associations`
`ntp server`

ntp server

Specifies the Network Timing Protocol (NTP) server to synchronize the time of a day with.

Command Syntax **[no] ntp server <*ipAddress*>| <*word*> [version <*version*>] [key <*key*>] [prefer] [iburst] [burst]**

Command Modes Configuration Mode `(config)#`

Syntax Description

ipAddress	IP address of the server to synchronize with.
name	Hostname of the server to synchronize with.
version	NTP version number to be used to communicate with the peer. The range is 1 to 4.
key	Key used to encrypt NTP packets. The range is 1 to 65534.
prefer	Marks the server as preferred.
iburst	Specifies that when the server is unreachable, a burst of packets should be sent rather than just one.
burst	Specifies that when the server is unreachable, a burst of packets should be sent rather than just one.

Command Default This command has no default values.

Examples

```
(config) #ntp server SERVER1 version 1 key 1
(config) #ntp server 10.1.1.10 version 1 key 1
```

Revision 1.0.1

Related Commands

`show ntp-associations`

`ntp peer`

password

Changes current user password.

Command Syntax	**password <*password*>**	
Command Modes	Configuration Mode	`(config)#`
Syntax Description	`password`	New password for current user.
Command Default	This command has no default values.	
Examples	#password PASSWORD1	
Revision	1.0.1	
Related Commands		

radius-server

Allows managing radius-server settings.

Command Syntax

[no] radius-server {hostname <*hostname*> | ip-address <*ipAddress*>} port <*portNumber*> [timeout <*seconds*> [key <*secret*>]]|[key <*secret*>]

Command Modes	Configuration Mode	`(config)#`
Syntax Description	*hostname*	Adds or modifies radius-server with specified hostname.
	ipAddress	Configures the IP address of the server to synchronize with.
	portNumber	
	seconds	Radius-server connection timeout (in seconds).
	secret	Radius server authentication key.
Command Default	This command has no default values.	

Examples

```
(config)#radius-server hostname HOSTNAME timeout 10 key
KEYWORD
(config)#no radius-server hostname HOSTNAME
```

Revision 1.0.1

Related Commands

`show radius-server`

tacacs-server

Allows managing TACACS server settings.

Command Syntax

[no] tacacs-server {hostname <*hostName*> | ip-address <*ipAddress*>} port <*portNumber*> [timeout <*timeout*> [key <*key*>]]|[key <*key*>]

Command Modes

Configuration Mode `(config)#`

Syntax Description

hostname *hostName*	Configures fully qualified domain name of the TACACS server host.
ip-address *ipAddress*	Configures the IP address of the TACACS server host.
port *portNumber*	
timeout *timeout*	Configures TACACS server connection timeout (in seconds). The range is 1-60.
key *key*	Manages TACACS server authentication key.

Command Default

This command has no default values.

Examples

```
(config) #tacacs-server ip-address 1.1.1.1 timeout 10
(config) #tacacs-server ip-address 1.1.1.1 timeout 60 key
authenKey
```

Revision

1.0.1

Related Commands

`show tacacs-server`

username authentication

Changes the settings of the user. The **no** form of the command deletes the user from the system.

Command Syntax

[no] username <*username*> authentication {local | remote} [password <*password*>][shell {bash | cli | xml-rpc}] [privilege {user | priv | admin}]

Command Modes

Configuration Mode `(config)#`

Syntax Description

username	Username to manage setting for.
local	Authentication as a local user.
remote	Authentication as a remote user.
password	Sets password for the specified user.
password	Password that will be set.

shell	Creates a new user in the system.
bash	Creates a local user which will use ‘bash’ as a default shell after login.
cli	Creates a local user which will use ‘cli’ as the default shell after login.
xml-rpc	Creates a local user which will use ‘xml-rpc’ as the default shell after login.
privilege	Specifies the privilege level of the user, that is specific access and ability permissions assigned to the user.
user	Sets simple user privileges.
priv	Allows the user to change the platform configuration.
admin	Sets administrative privileges for the specified user.

Command Default This command has no default values.

Examples

```
#username name.surname authentication local password
passphrase shell bash privilege admin
```

Revision 1.0.1

Related Commands

`show username`

5.4 Management Port Interface Mode

duplex

Sets the concurrency of the bidirectional communication paths for the management interface. The **no** form of this command removes the link duplex mode.

Command Syntax **[no] duplex half|full**

Command Modes Interface Configuration Mode

```
#configure
(config) #interface mgmt-ethernet
(config-if)#
```

Syntax Description		
	half	Enables bidirectional communications but not concurrently.
	full	Enables full concurrency for both directions.

Command Default The default duplex value is **full.**

Examples

```
(config-if)#duplex half
(config-if)#duplex full
(config-if)#no duplex
```

Revision 1.0.1

Related Commands

show interface mgmt-ethernet

ip default-gateway

Configures the gateway IP address for the management port. The **no** form of this command unsets the gateway IP address.

Command Syntax **[no] ip default-gateway <*ipAddress*>**

Command Modes Interface Configuration Mode

```
#configure
(config) #interface mgmt-ethernet
(config-if)#
```

Syntax Description		
	ipAddress	Gateway IP address.

Command Default This command has no default values.

Examples

```
(config-if)#ip default-gateway 1.1.1.1
(config-if)#no ip default-gateway
```

Revision 1.0.1

Related Commands

show interface mgmt-ethernet

hostname

Configures the host name for the management port. The **no** form of this command removes the host name.

Command Syntax **[no] hostname <*hostName*>**

Command Modes

Interface Configuration Mode

```
#configure
(config) #interface mgmt-ethernet
(config-if)#
```

Syntax Description

hostName	Host name for the management port.

Command Default

Examples

```
(config-if)#hostname HOSTNAME
(config-if)#no hostname
```

Revision 1.0.1

Related Commands

`show interface mgmt-ethernet`

ip address

Configures the IP address for the management port.

Command Syntax **ip address {<*ipAddress*> <*subnetMask*>} | dhcp**

Command Modes

Interface Configuration Mode

```
#configure
(config) #interface mgmt-ethernet
(config-if)#
```

Syntax Description

ipAddress	IP address for the management port.
subnetMask	Subnet mask for the management port.
dhcp	Gets an IP address for the management port from the DHCP server.

Command Default This command has no default values.

Examples

```
(config-if)#ip address 1.1.1.1 255.255.255.0
 (config-if)#ip address dhcp
```

Revision 1.0.1

Related Commands

`show interface mgmt-ethernet`

mtu

Configures the maximum frame size, in bytes, that a port can transmit. Larger frames must be fragmented before transmission. The parameter is Maximum Transmission Unit (MTU). The **no** form of the command sets the maximum frame size to default.

Command Syntax **[no] mtu <*mtu*>**

Command Modes Interface Configuration Mode

```
#configure
(config) #interface mgmt-ethernet
(config-if)#
```

Syntax Description *mtu* Maximum Transmission Unit. The range is `330` to 9210

Command Default The default value for all ports is 1518.

Examples

```
(config-if)#mtu 1000
(config-if)#no mtu
```

Revision 1.2

Related Commands

`show interface mgmt-ethernet`

shutdown

Controls the administrative state of the management port.

Command Syntax **[no] shutdown**

Command Modes Interface Configuration Mode

```
#configure
(config) #interface mgmt-ethernet
(config-if)#
```

Syntax Description This command does not have any parameters or key words.

Command Default Operational (not shutdown)

Examples

```
(config-if)#shutdown
(config-if)#no shutdown
```

Revision 1.0.1

Related Commands

`show interface mgmt-ethernet`

speed

Sets the speed of the port in megabits/s (Mbps). The **no** command sets the port speed to non-negotiable and to 0 Mbps.

Command Syntax **speed {<*speed*> | auto | nonegotiate}**

no speed

Command Modes Interface Configuration Mode

```
#configure
(config) #interface mgmt-ethernet
(config-if)#
```

Syntax Description

speed	Sets speed value. The no form of the command sets default value for the interface speed configuration.
speed	Port speed in Mbps. The options are 1000, 2500, 10000, 40000.
auto	Enables autonegotiation on the interface. This is the default setting.
nonegotiate	Disables the autonegotiation on the interface. To restore autonegotiation, set the autonegotiate on the interface to Enable.

Command Default The default port speed for all ports is 1000.

Examples

```
(config-if)#speed 10
(config-if)#speed 100
(config-if)#speed 1000
(config-if)#speed auto
(config-if)#speed nonegotiate
(config-if)#no speed
```

Revision 1.2

Related Commands

`show interface mgmt-ethernet`

threshold metric

Configures the interface subsystem thresholds. The key word **metric** specifies for which indicator threshold is being configured. The **no** form of the command is used to clear interface subsystem thresholds.

Command Syntax

threshold metric {tx-bytes | rx-bytes | tx-packets | rx-packets | tx-errors | rx-errors} { {hits <_hits_ **>} | {type { { warning { {low <**_low_**> [high <**_high_**>]} | {high <**_high_**> [low <**_low_**>]} } } | { failure { {low <**_low_**> [high <**_high_**>]} | {high <**_high_**> [low <**_low_**>]} } } } } }**

no threshold metric {tx-bytes | rx-bytes | tx-packets | rx-packets | tx-errors | rx-errors} [hits | type { {warning [{low [high]} | {high [low]}]} | {failure [{low [high]} | {high [low]}]} }]

Command Modes

Interface Configuration Mode

```
#configure
(config) #interface mgmt-ethernet
(config-if)#
```

Syntax Description

tx-bytes	Configures interface subsystem thresholds for the transmitted bytes.
rx-bytes	Configures interface subsystem thresholds for the received bytes.
tx-packets	Configures interface subsystem thresholds for the transmitted packets.
rx-packets	Configures interface subsystem thresholds for the received packets.
tx-errors	Configures interface subsystem thresholds for the transmitted corrupt packets.
rx-errors	Configures interface subsystem thresholds for the received corrupt packets.
low	Configures the lower bound of acceptable values for the warning or failure threshold.

low	Lower bound of acceptable values.
high	Configures the upper bound of acceptable values for the warning or failure threshold.
high	Upper bound of acceptable values.
hits	Delays generating a WARNING or FAILURE log until the threshold has been crossed ‘hits’ number of times.
hits	Delay of creating the notification until the threshold has benn passed.
type warning|failure	Specifies which threshold is being configures, either WARNING or FAILURE. If not specified, the configured threshold defaults to WARNING.

Command Default

Examples

```
(config-if)#threshold metric tx-packets low 10 high 100 type warning
```

Revision 1.2

Related Commands

`show interface mgmt-ethernet thresholds`

6. Layer 2 Commands

This section covers the Data Link Layer (layer 2) commands for the User mode, Privileged mode, and Global Configuration mode.

6.1 User Mode Commands

This topic covers the User mode commands for the Data Link Layer (layer 2) environment. The User mode allows you to display some configuration parameters and allows you to access the Privileged mode.

show interface (User)

Shows the configuration of all interfaces (ports) or of the specified interface. The output includes port configuration information and port statistics.

Command Syntax **show interface [**<*interfaceName*>**]**

Command Modes User Execution Mode >

Syntax Description *interfaceName* Name of the port interface. For example, **xe1**.

Examples

```
>show interface
>show interface xe1
```

System Response The output fields for **interface** are as follows:

Field	Description
Port	The system generated, fixed and unique logical port identifier value.
Name	Port name. For example, **xe1**.
Description	Description of the interface.
MAC Address	MAC address of the port.
Type	Physical port type.
Administrative Mode	State of the port.
Operational Status	Operational status of the port.
Auto Negotiate	Port auto-negotiation mode.
Speed	Port speed in kbits/s.
Duplex	Concurrency of the bidirectional communication paths for the interface.
Flow Control	Whether the interface processes received pause frames or sends pause frames.
Maximum Frame Size	Current state of the parameter.
PVID	Port VLAN identifier.
PVPT	Port VLAN priority.
Learning Mode	The method the port uses to learn MAC addresses.
Ingress Filtering	Current state of ingress filtering capability on the port.
Discard Mode	The packet discard mode for the port.
Cut Through	The cut-through interface option allows packets to be transmitted on a port before the entire packet is received.
IGMP Enable	Internet Group Management Protocol (IGMP) mode.

Mac Mode	Port MAC Mode (Normal/Fanout).

Revision 1.0.1

Related Commands

interface (modes)
show statistics
show interface (Privileged)

show mac-address-table (User)

Shows the forwarding database for the system or for a specific MAC address.

Command Syntax **show mac-address-table [***macAddress***]**

Command Modes User Execution Mode >

Syntax Description *macAddress* MAC address.

Examples

```
>show mac-address-table 00:00:67:00:00:01
>show mac-address-table
```

System Response The output fields for **mac-address-table** are as follows:

Field	Description
Port	The system generated, fixed and unique logical port identifier value.
MacAddress	MAC address of the port.
Vlan	VLAN identifier
Type	Static or Dynamic
Total MAC addresses count	Number of MAC addresses.
Static MAC addresses count	Number of static MAC addresses.
Dynamic MAC addresses count	Number of dynamic MAC addresses.

Revision 1.0.1

Related Commands

mac-address-table
show mac-address-table (Privileged)

show mac-address-table static

Shows static forwarding database entries.

Command Syntax **show mac-address-table static [***macAddress***]**

Command Modes User Execution Mode >

Syntax Description

static	Shows static forwarding database entries.
macAddress	MAC address.

Examples

```
>show mac-address-table static 00:00:67:00:00:01
>show mac-address-table static
```

System Response

The output fields for **mac-address-table static** are as follows:

Field	Description
Port	The system generated, fixed and unique logical port identifier value.
MacAddress	MAC address of the port.
Vlan	VLAN identifier
Total MAC addresses count	Number of MAC addresses.
Static MAC addresses count	Number of static MAC addresses.
Dynamic MAC addresses count	Number of dynamic MAC addresses.

Revision 1.2

Related Commands

`mac-address-table`
`show mac-address-table (Privileged)`

show monitor

Shows interface monitor.

Command Syntax **show monitor**

Command Modes User Execution Mode >

Examples

```
>show monitor
```

System Response

The output fields for **show monitor** are as follows:

Field	Description
Mode	Status and type of interface mirroring mode.
Preserved mode	Global interface preserve monitoring mode.
Source interface	Interface name or interface names list separated by dash or commas that you want to add for mirroring.
Destination interface	Name of the destination interface.
Mode	Mode for egress and ingress packets mirroring.

Revision 1.0.1

Related Commands

show terminal

Shows terminal session configuration.

Command Syntax **show terminal**

Command Modes User Execution Mode >

Command Default Default terminal length is 24.

Examples

```
>show terminal
```

System Response The output fields for **show terminal** are as follows:

Field	Description
Terminal Length	Number of lines used to paginate command output.

Revision 1.1

Related Commands

```
terminal length (User)
terminal length (Privileged)
show terminal (Privileged)
```

show version

Shows the current software version of the CLI.

Command Syntax **show version**

Command Modes User Execution Mode >

Examples

```
>show version
```

Revision 1.0.1

Related Commands

```
show system
show running-config
```

show vlan

Shows the VLAN configuration for all VLANs or a specific VLAN.

Command Syntax **show vlan** [*vlanId*]

Command Modes User Execution Mode >

Syntax Description *vlanId* VLAN identifier. The range is 1 to 4094.

Examples

```
>show vlan 1
>show vlan
```

System Response The output fields for **vlan** are as follows:

Field	Description
Name	Name of the VLAN.
Port	Port number.
Tagged	Whether the traffic is tagged or untagged.
Vlan	VLAN number.

Revision 1.0.1

Related Commands

`interface`
`switchport`
`vlan-database`
`wrr-queue`
`show vlan (Privileged)`

terminal length

Configures terminal length.

Command Syntax **[no] terminal length <*terminalLength*>**

Command Modes User Execution Mode >

Syntax Description *terminalLength* `Value for terminal length.`

Command Default Default value for [no] command is 24.
0 - sets unlimited terminal length.

Examples

```
>terminal
>terminal length 0
>no terminal length
```

System Response The output fields for **terminal length** are as follows:

Field	Description
Terminal Length	Number of lines used to paginate command output.

Revision 1.1

Related Commands

`terminal length (Privileged)`
`show terminal (Privileged)`
`show terminal (User)`

6.2 Privileged Mode Commands

clear mac-address-table

Deletes entries from the MAC address table.

Command Syntax **clear mac-address-table**

Command Modes Privileged Mode

```
>enable
#
```

Examples

```
#clear mac-address-table
```

Revision 1.0.1

Related Commands

show mac-address-table (User)
show mac-address-table (Privileged)
mac-address-table

delete saved-config

Deletes saved configuration with specified name.

Command Syntax **delete saved-config <*name*>**

Command Modes Privileged Mode

```
>enable
#
```

Syntax Description *name* Name or saved configuration to delete.

Examples

```
Switch #show saved-configs

Version                             Date
---------------------------------- -------------------------
baseline-cfg                        Tue Nov 26 16:08:52 2013
default-cfg                         Tue Nov 26 14:26:05 2013

Switch #save config AAAAA

Switch #show saved-configs

Version                             Date
----------------------------------- ------------------------
baseline-cfg                        Tue Nov 26 16:08:52 2013
AAAAA                               Wed Nov 27 14:10:58 2013
default-cfg                         Tue Nov 26 14:26:05 2013

Switch #delete saved-config AAAAA
Switch #show saved-configs

Version                             Date
----------------------------------- ------------------------
baseline-cfg                        Tue Nov 26 16:08:52 2013
```

```
default-cfg                                 Tue Nov 26 14:26:05 2013
```

Revision 1.2

Related Commands

`#show saved-configs`
`#save config`

vlan-database

Enters the vlan configuration mode (vlan) from the privileged mode (#). This mode enables the creation and deletion of VLANs.

Command Syntax **vlan-database**

Command Modes Privileged Mode

```
#vlan-database
(vlan) #
```

Examples

```
#vlan-database
(vlan) #?
(vlan) #exit
#
```

Revision 1.0.1

Related Commands

`vlan`
`show vlan`
`wrr-queue`
`switchport`
`exit`

show access-groups

Displays the list of ACL groups.

Command Syntax **show access-groups** [<*InterfaceName*>]

Command Modes Privileged Mode #

Syntax Description

InterfaceName	Name of an interface port. For example, **xe1**.

Command Default This command has no default settings.

Examples

```
#show access-groups xe1
#show access-groups
```

System Response The output fields are as follows:

Field	Description
Interface	Name of the port interface.
Access Group	Number of the ACL group.
Stage	

Revision 1.0.1

Related Commands

`access-list`
`access-group`

show access-lists

Shows all access lists in the system or the specified access list. If there are no access lists or the specified access list does not exist, no output is provided.

Command Syntax **show access-lists [**<*accessListNumber*>**|{rules|expressions|statistics|actions [**<*accessListNumber*>**]}]**

Command Modes Privileged Mode #

Syntax Description

accessListNumber	Number of the access list to show information for.
rules	Shows ACL rules.
expressions	Shows ACL expressions.
statistics	Shows ACL statistics information.
actions	Shows ACL actions.

Command Default This command has no default settings.

Examples

```
#show access-lists
#show access-lists 1
```

```
#show access-lists rules
#show access-lists rules 1
#show access-list expressions
#show access-list expressions 1
```

System Response

The output fields for **access-lists** are as follows:

Field	Description
ACL number	Access list number.
Stage	State of the packet processing to apply rule on.
Action	Number of ACL rule.
L4 Src Port	L4 Src Port.
EtherType	EtherType.
IP Protocol	Ip Protocol.
TTL	Time To Live.
IP type	

The output fields for **access-list rules** are as follows:

Field	Description
Rule ID	Number of ACL rule.
Status	Status of the rule (Disabled or Enabled)
Priority	Rule priority. Rule with higher priority value takes precedence over lower priority value.
Stage	State of the packet processing to apply rule on.
Action ID	An action ID associated with specified rule.
Expression ID	An expression ID associated with specified rule.

The output fields for **access-list expressions** are as follows:

Field	Description
Expression ID	The expression ID.
Field	The packet field mnemonic.
Data	The expected result of anding the field with the mask (field AND mask).
Mask	The mask to bitwise and the field with.

The output fields for **access-list actions** are as follows:

Field	Description
Action ID	The action ID.
Action	The actual action mnemonic.
Parameters	Action parameter.

The output fields for **access-list statistics** are as follows:

Field	Description
Rule ID	Number of ACL rule.
Match Packets	Number of packets that the rule is applied to.
Match Octets	Number of octets that the rule is applied to.

Revision	1.0.1
Related Commands	access-list access-group

show access-lists policers

Shows a specified ACL policer. If parameter value is not specified, the command shows all configured ACL policers.

Command Syntax	**show access-lists policers [<*policerId*>]**	
Command Modes	Privileged Mode	#
Syntax Description	**policers**	Show ACL policers.
	policerId	Policer ID.
Command Default	This command has no default settings.	

Examples

```
#show access-lists policers

ID ..................................... 1
Committed buffer capacity limit ......... 3
Committed rate limit .................... 4
Committed action ........................ SetVlanPri
Committed action parameters ............. 2
Excess buffer capacity limit ............ 5
Excess rate limit ....................... 6
Excess action ........................... TrapToCpu
Excess action parameters ................ N/A

ID ..................................... 2
Committed buffer capacity limit ......... 3
Committed rate limit .................... 4
Committed action ........................ DoNothing
Committed action parameters ............. N/A
Excess buffer capacity limit ............ 5
Excess rate limit ....................... 6
Excess action ........................... Drop
Excess action parameters ................ N/A

#show access-lists policers 1
ID ..................................... 1
Committed buffer capacity limit ......... 1
Committed rate limit .................... 1
Committed action ........................ SetVlanPri
Committed action parameters ............. 1
Excess buffer capacity limit ............ 1
Excess rate limit ....................... 1
Excess action ........................... SetVlanPri
Excess action parameters ................ 1
```

System Response The output fields for **access-lists policers** are as follows:

Field	Description
ID	Policer ID.

Committed buffer capacity limit	Committed buffer capacity limit for storing queued packets.
Committed rate limit	Committed rate limit in kbps for traffic.
Committed action	Committed rate/capacity action.
Committed action parameters	Excess rate action parameter.
Excess buffer capacity limit	Excess buffer capacity limit for storing queued packets.
Excess rate limit	Excess rate limit in kbps for traffic.
Excess action	Excess rate/capacity action.
Excess action parameters	Excess rate action parameters.

Revision 1.2

Related Commands

show channel-group

Displays status information for the channel groups.

Command Syntax

show channel-group [<*portChannel*>] [{admin | neighbor}]

show channel-group[<portChannel>] detail

Command Modes Privileged Mode #

Syntax Description

portChannel	Port-channel ID to show information for.
admin	Displays the administrative configuration.
neighbour	Shows channel group neighbor configuration.
detail	Shows detailed information about channel groups.

Command Default This command has no default settings.

Examples

```
#show channel-group
#show channel-group 3800
#show channel-group 3800 neighbor
#show channel-group neighbor
#show channel-group 3800 admin
#show channel-group admin
#show channel-group detail
#show channel-group 3800 detail
```

System Response The output fields for **channel-group** are as follows:

Field	Description
Port Channel	Port channel number
Port	The system generated, fixed and unique logical port identifier value.
Operational Conflict	Indicates this port’s operational conflict state, which is often due to the keys mismatching
Operational Port Key	The operational key of the LAG this port belongs too.

Operational Port Status	The operational values of the Actor's state parameters, presented as individual bits within a bit string starting with the most significant bit.
LACP Administrative Status	Shows whether this port is LACP enabled or not.
Churn Detection Status	Indicates whether this port is churning while trying to join its LAG.
Traffic Send Status	
Port Enabled	Indicates whether the port is enabled or not.
Selected Mode	The selected state of the port as determined by the Selection Logic State Machine.
Received Counter.	Counts the number of control packets (LACPDUs) received by the port.
Transmit Counter	Counts the number of control packets (LACPDUs) transmitted by the port.

The output fields for **channel-group admin** are as follows:

Field	Description
Port Channel	Port channel number.
Port	
Priority	The operational priority of the system that this port is connected to.
Key	The administratively set key corresponding to the LAG this port is under. If it is changed to a key not belonging to the LAG the port is under, you will have an operational conflict.
Aggregation	The aggregation mode for a channel group.
Active	Specifies whether LACP is enabled unconditionally.
Time	The interval between the transmission of LACP PDUs.
Synchronization	Specifies if the configuration of the port is synchronized with the port channel configuration.
Collecting	Specifies whether the local port is collecting.
Distributing	Specifies whether the local port is distributing.
Defaulted	Specifies whether the local port is defaulting.
Expired	Specifies whether the local port is expired.
Partner System	Indicates the unique, globally administered MAC address.
Partner System Priority	Partner Operational Port Priority
Partner Port State	The operational state of the port that this local port (actor) is connected to.
Partner Port Number	The operational key of the port that this local port (actor) is connected too.

The output fields for **channel-group neighbour** are as follows:

Field	Description
Port Channel	Port channel number.
Port	The system generated, fixed and unique logical port identifier value.
System	Indicates the unique, globally administered MAC address.
System Priority	The operational priority of the system that this port is connected to.
Port State	The operational state of the port that this local port (actor) is connected to.
Port Number	The operational key of the port that this local port (actor) is connected too.
Key	The administratively set key corresponding to the LAG this port is under. If it is changed to a key not belonging to the LAG the port is under, you will have an operational conflict.

	Port Priority	The operational priority of the system that this port is connected to.
	Churn Detection Status	Indicates whether this port is churning while trying to join its LAG.
Revision	1.2	
Related Commands	channel-group	

show clock

Shows the system date and time zone.

Command Syntax	**show clock**	
Command Modes	Privileged Mode	#
Command Default	This command has no default settings.	

Examples

```
#show clock

05:59:29.770072 None 2000-01-02
```

Revision 1.0.1

Related Commands

show dcb app

Displays DCB (Data center bridging) application data.

Command Syntax	**show dcb app {local status|map}|{remote status|map}|status|map**	
Command Modes	Privileged Mode	#
Syntax Description	**local**	Displays the local application data.
	remote	Displays the remote application data.
	status	Displays the status application data.
	map	Displays the map application data.
Command Default	This command has no default settings.	

Examples

```
#show dcb app map
#show dcb app status
#show dcb app local map
```

```
#show dcb app remote map
#show dcb app local status
#show dcb app remote status
```

System Response The output fields for **dcb app** include local and remote parameters.

Field	Description
Interface	The system generated, fixed and unique logical port identifier value(interface name).
Selector	Indicates the contents of the protocol object 1: Ethertype. 2: Well Known Port number over TCP, or SCTP. 3: Well Known Port number over UDP, or DCCP. 4: Well Known Port number over TCP, SCTP, UDP, and DCCP.
Protocol	The protocol indicator of the type indicated by selector.
Priority	The priority code point that should be used in frames transporting the protocol indicated by selector and priority.
Willing	Indicates if the local system is willing to accept the Application Priority configuration of the remote system.
Error Alarm	Indicates if a configuration error alarm is active.
Total TX TLVs	Application Priority TLVs transmitted counter.
Total RX TLVs	Application Priority TLVs received counter.

Revision 1.0.1

Related Commands

dcb

show dcb cn

Displays DCB (Data center bridging) congestion notification data.

Command Syntax **show dcb cn [local | remote]**

Command Modes Privileged Mode #

Syntax Description

local	Displays the local congestion notification data.
remote	Displays the remote congestion notification data.

Command Default This command has no default settings.

Examples

```
#show dcb cn local
#show dcb cn remote
```

System Response The output fields for **dcb cn** include local and remote parameters.

Field	Description
Interface	The system generated, fixed and unique logical port identifier value.
Local Port	The system generated, fixed and unique logical port identifier value.

CNPV Supported	Indicates if CNPV is supported for the corresponding priority.
CNPV Ready	Indicates if CNPV is ready for the corresponding priority.
Error Alarm	Indicates if a configuration error alarm is active.
Total TX TLVs	CN configuration TLVs transmitted counter.
Total RX TLVs	CN configuration TLVs received counter.
Valid	Indicates the validity of the entry.

Revision 1.0.1

Related commands

dcb

show dcb dcbx

Displays DCB (Data center bridging) dcb exchange data.

Command Syntax **show dcb dcbx [{neighbors [interface <*interfaceName*>]} | {interface <*interfaceName*>]**

Command Modes Privileged Mode #

Syntax Description

neighbors	Shows learned information about DCB on all neighbors
interface	Shows learned information about DCB on selected interfaces.
interfaceName	Specified interface learned information.

Command Default This command has no default settings.

Examples

```
#show dcb dcbx local
#show dcb dcbx remote
```

System Response The output fields for **dcb dcbx** include local and remote parameters.

Field	Description
Interface	The system generated, fixed and unique logical port identifier value and the second of two primary keys for this table
Administrative Status	The administratively desired status of the local DCBx agent. When disabled, the DCBx agent will not transmit or receive DCBx frames on this port. If there is remote systems information which is received on this port and stored in other tables, before the port becomes disabled, then the information will naturally age out. When enabled, the DCBx agent will transmit and receive DCBx frames on this port.
PFC	Determines whether the IEEE 802.1 organizationally defined Priority-based Flow Control TLV transmission is allowed on a given LLDP transmission capable port. The value of this object is restored from non-volatile storage after a re-initialization of the management system.
ETS Conf	Determines whether the IEEE 802.1 organizationally defined ETS Configuration TLV transmission is allowed on a given LLDP transmission capable port. The value of this

	object is restored from nonvolatile storage after a re-initialization of the management system.
ETS Reco	Determines whether the IEEE 802.1 organizationally defined ETS Recommendation TLV transmission is allowed on a given LLDP transmission capable port. The value of this object is restored from nonvolatile storage after a re-initialization of the management system.
APP	Determines whether the IEEE 802.1 organizationally defined Application Priority TLV transmission is allowed on a given LLDP transmission capable port. The value of this object is restored from nonvolatile storage after a re-initialization of the management system.
CN	Determines whether the IEEE 802.1 organizationally defined Congestion Notification TLV transmission is allowed on a given LLDP transmission capable port. The value of this object is restored from nonvolatile storage after a re-initialization of the management system.
Multiple Peers Alarm	Multiple Peers alarm
Active Protocol Version	Current configured DCBX protocol version, to be used when sending/receiving DCBX frames on port.
Administrative Protocol Version	Admin configured DCBX protocol version, to be used when sending/receiving DCBX frames on port.

The output fields for **dcb dcbx neighbors interface** are as follows:

Field	Description
Port	The index value used to identify the port component (contained in the local chassis with the LLDP agent) associated with this entry. The lldpRemLocalPortNumidentifies the port on which the remote system information is received.
Remote Port	The object represents an arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated remote system.
Remote MAC Address	The value used to identify the destination MAC address associated with this entry.
Time Filter	A TimeFilter for this entry.
Valid Entry	Indicates that this entry is valid.

The output fields for **dcb dcbx interface** are as follows:

Field	Description
Port	The system generated, fixed and unique logical port identifier value and the second of two primary keys for this table.
Administrative Status	The administratively desired status of the local DCBx agent. When disabled, the DCBx agent will not transmit or receive DCBx frames on this port. If there is remote systems information which is received on this port and stored in other tables, before the port becomes disabled, then the information will naturally age out. When enabled, the DCBx agent will transmit and receive DCBx frames on this port.
PFC	Determines whether the IEEE 802.1 organizationally defined Priority-based Flow Control TLV transmission is allowed on a given LLDP transmission capable port. The value of this object is restored from non-volatile storage after a re-initialization of the management system.
ETS Conf	Determines whether the IEEE 802.1 organizationally defined ETS Configuration TLV transmission is allowed on a given LLDP transmission capable port. The value of this object is restored from nonvolatile storage after a re-initialization of the management system.

ETS Reco	Determines whether the IEEE 802.1 organizationally defined ETS Recommendation TLV transmission is allowed on a given LLDP transmission capable port. The value of this object is restored from nonvolatile storage after a re-initialization of the management system.
APP	Determines whether the IEEE 802.1 organizationally defined Application Priority TLV transmission is allowed on a given LLDP transmission capable port. The value of this object is restored from nonvolatile storage after a re-initialization of the management system.
CN	Determines whether the IEEE 802.1 organizationally defined Congestion Notification TLV transmission is allowed on a given LLDP transmission capable port. The value of this object is restored from nonvolatile storage after a re-initialization of the management system.
Multiple Peers Alarm	Multiple Peers alarm
Active Protocol Version	Current configured DCBX protocol version, to be used when sending/receiving DCBX frames on a port.
Administrative Protocol Version	Admin configured DCBX protocol version, to be used when sending/receiving DCBX frames on a port.

Revision 1.0.1

Related Commands

dcb

show dcb ets-conf

Displays DCB (Data center bridging) enhanced transmission selection (ETS) configuration data.

Command Syntax **show dcb ets-conf [local | remote]**

Command Modes Privileged Mode #

Syntax Description

local	Displays the local ETS configuration data.
remote	Displays the remote ETS configuration data.

Command Default This command has no default settings.

Examples

```
#show dcb ets-conf local
#show dcb ets-conf remote
```

System Response The output fields for **dcb ets-conf** include local and remote parameters.

Field	Description
Interface	The system generated, fixed and unique logical port identifier value.
Local Port	The system generated, fixed and unique logical port identifier value.
Willing	Indicates if the local system is willing to accept the ETS configuration recommended by the remote system.
CBS	Indicates if the credit-based shaper Traffic Selection Algorithm is supported on the remote system.
Maximum TCs	Indicates the number of Traffic Classes supported on the remote system. A value of 0 indicates that 8Traffic Classes

	are supported.
Error Alarm	Indicates if a configuration error alarm is active.
TX TLVs	ETS configuration TLVs transmitted counter
RX TCs	ETS configuration TLVs received counter
Bandwidth	Each octet corresponds to one traffic class. The first octet corresponds to traffic class 0, the second to traffic class 1, and so on. Each octet contains the bandwidth in percent to be allocated to the traffic class. Valid values are between 0 and 100 inclusive. The total of all eight octets must equal 100. Note that an octet string is used instead of a table to enable atomic programming of these values which is required to fulfill the requirement that they always total to 100.
Algorithm	Indicates a traffic class to traffic selection algorithm assignment. 0: Strict Priority 1: Credit-based shaper 2: Enhanced transmission selection 3-254: Reserved for future standardization 255: Vendor specific
Priority Assignment	Indicates the traffic class to which the priority is assigned. 15 indicates that the priority is not assigned to any traffic class.

Revision 1.0.1

Related Commands

`dcb`

show dcb ets-reco

Displays DCB (Data center bridging) enhanced transmission selection (ETS) recommended data.

Command Syntax **show dcb ets-reco [local | remote]**

Command Modes Privileged Mode #

Syntax Description

local	Displays the local ETS recommended data.
remote	Displays the remote ETS recommended data.

Command Default This command has no default settings.

Examples

```
#show dcb ets-reco local
#show dcb ets-reco remote
```

System Response The output fields for **dcb ets-reco** include local and remote parameters.

Field	Description
Interface	The system generated, fixed and unique logical port identifier value.
Local Port	The system generated, fixed and unique logical port identifier value.
Willing	Indicates if the local system is willing to accept the ETS configuration recommended by the remote system.
CBS	Indicates if the credit-based shaper Traffic Selection Algorithm is supported on the remote system.

Maximum TCs	Indicates the number of Traffic Classes supported on the remote system. A value of 0 indicates that 8Traffic Classes are supported.
Error Alarm	Indicates if a configuration error alarm is active.
TX TLVs	ETS configuration TLVs transmitted counter
RX TCs	ETS configuration TLVs received counter
Bandwidth	Each octet corresponds to one traffic class. The first octet corresponds to traffic class 0, the second to traffic class 1, and so on. Each octet contains the bandwidth in percent to be allocated to the traffic class. Valid values are between 0 and 100 inclusive. The total of all eight octets must equal 100. Note that an octet string is used instead of a table to enable atomic programming of these values which is required to fulfill the requirement that they always total to 100.
Algorithm	Indicates a traffic class to traffic selection algorithm assignment. 0: Strict Priority 1: Credit-based shaper 2: Enhanced transmission selection 3-254: Reserved for future standardization 255: Vendor specific
Priority Assignment	Indicates the traffic class to which the priority is assigned. 15 indicates that the priority is not assigned to any traffic class.

Revision 1.0.1

Related Commands

`dcb`

show dcb pfc

Displays DCB (Data center bridging) Priority Flow Control (PFC) data.

Command Syntax **show dcb pfc [local | remote]**

Command Modes Privileged Mode #

Syntax Description

local	Displays the local PFC data.
remote	Displays the remote PFC data.

Command Default This command has no default settings.

Examples

```
#show dcb pfc local
#show dcb pfc remote
```

System Response The output fields for **dcb pfc** include local and remote parameters.

Field	Description
Interface	The system generated, fixed and unique logical port identifier value
Local Port	The system generated, fixed and unique logical port identifier value
Willing	Indicates if the local system is willing to accept the configuration recommended by the remote system.
MBC	Indicates if the local system is capable of bypassing MACsec processing when MACsec is disabled.

Capability	Indicates the number of traffic classes on the local device that may simultaneously have PFC enabled. Zero indicates no limitation, i.e. all available traffic classes may have PFC enabled. The default value is 1.
Enabled	Indicates if PFC is enabled on the corresponding priority. Value is formatted as binary list starting with priority 0 to priority 7 - 0,1,1,0,0,0,0,0 (1 and 2 are enabled). The "enabled" field takes only the string with only 1 in any one. The PFC feature supports only one priority-based flow control (PFC) queue, priority queue, for example: '0,0,0,1,0,0,0,0'.
Error Alarm	Indicates if a configuration error alarm is active.
Total TX TLVs	PFC TLVs transmitted counter
Total RX TLVs	PFC TLVs received counter

Revision 1.2

Related Commands

dcb

show dot1q-tunnel

Shows 802.1Q (QinQ) tunnel information.
802.1Q tunneling allows layer 2 VPN connectivity between sites by encapsulating 802.1Q trunk traffic inside another 802.1Q trunk.

Command Syntax

show dot1q-tunnel [interface {<*interfaceName*>| {port-channel <*portChannel*>}}]
show dot1q-tunnel {customer | provider} vlan mapping [interface {<*interfaceName*>| {port-channel <*portChannel*>}}]
show dot1q-tunnel encapsulation [interface {<*interfaceName*>| {port-channel <*portChannel*>}}]

Command Modes Privileged Mode #

Syntax Description

interface	Show 802.1Q tunnel configuration on the specified interface.
interfaceName	Interface to show information for.
port-channel	Show 802.1Q tunnel configuration on the specified port channel.
portChannel	Port channel to show 802.1Q tunnel configuration information for.
encapsulation	Displays 802.1Q tunnel stacked VLAN configuration.
vlan mapping	Displays 802.1Q tunnel VLAN mapping information.
customer	Displays 802.1Q tunnel customer VLAN mapping information.
provider	Displays 802.1Q tunnel provider VLAN mapping information.
interfaceName	Name of an interface port. For example, **xe1**.

Command Default This command has no default settings.

Examples

```
#show dot1q-tunnel interface xe1
#show dot1q-tunnel interface port-channel 3800
#show dot1q-tunnel customer vlan mapping
```

```
#show dot1q-tunnel customer vlan mapping interface xe1
#show dot1q-tunnel customer vlan mapping port-channel 3800
#show dot1q-tunnel encapsulation
#show dot1q-tunnel encapsulation interface xe1
#show dot1q-tunnel encapsulation port-channel 3800
```

System Response

The output fields for **dot1q-tunnel interface** are as follows:

Field	Description
Port	Port identifier
Mode	Displays the 802.1Q tunnel mode
TPID	Specifies the Tag Protocol Identifier

For **dot1q-tunnel encapsulation** the output fields are the following:

Field	Description
Port	Port identifier
Provider VLAN	Service provider VLAN identifier
Provider VLAN Priority	Service provider VLAN priority

The output fields for **dot1q-tunnel vlan mapping** are as follows:

Field	Description
Port	Port identifier
Provider VLAN	Service provider VLAN identifier
Customer VLAN	Customer VLAN identifier
Customer VLAN Priority	Customer VLAN priority
Provider VLAN Priority	Service provider VLAN priority

Revision

1.2

Related Commands

`encapsulation dot1q`

show errdisable

Shows the ErrDisable reasons and for which reason the autorecovery feature has been enabled.

Command Syntax

show errdisable {detect | recovery}

Command Modes

Privileged Mode	#

Syntax Description

detect	Shows the ErrDisable feature detection status.
recovery	Shows the ErrDisable reasons, and for which reason the autorecovery feature has been enabled.

Command Default

Examples

```
#show errdisable recovery
#show errdisable detect
```

System Response

The output fields for **errdisable recovery** are as follows:

Field	Description
ErrDisable Status	Shows current global ErrDisable status.
Port recovery interval	Auto-recovery timeout value in seconds.
Udld status	Timer to recover from the Unidirectional Link Detection (UDLD) status.
BPDU guard status	Bridge Protocol Data Unit guard status.

The output fields for **errdisable detect** are as follows:

Field	Description
Application	Name of the application that can set this error on a port.
Port Error Name	Application specific port error.
Detection Status	Defines if recovery mechanism is available for this appError.
Recovery Status	Defines if recovery mechanism is enabled for specific appError.

Revision 1.2

Related Commands

show lldp

Shows the Link Layer Discovery Protocol (LLDP) parameters for each interface (port).

Command Syntax

show lldp
show lldp traffic interface <*interfaceName***>**
show lldp interface <*interfaceName* **>**
show lldp neighbors [interface <*interfaceName***>]**

Command Modes Privileged Mode #

Syntax Description

traffic interface	Displays the local lldp statistics for interface.
interface	Displays the local Lldp parameters for interface (also includes local management information).
neighbors interface	Displays neighbors information (also includes neighbors management information).
interfaceName	Name of an interface port. For example, **xe1**.

Command Default This command has no default settings.

Examples

```
#show lldp
#show lldp traffic interface xe1
#show lldp interface xe1
#show lldp neighbors interface
#show lldp neighbors interface xe1
```

System Response The output fields for **lldp** are as follows:

Field	Description
Message Transmit Interval	The interval at which LLDP frames are transmitted on behalf of this LLDP agent.
Message Transmit Hold	The time-to-live value expressed as a multiple of the Tx

Multiplier	Interval object. The actual time-to-live value used in LLDP frames, transmitted on behalf of this LLDP agent, can be expressed by the following formula: TTL= min(65535,(Tx Interval * Tx Hold Multiplier)).
Transmit Re-init Delay	Indicates the delay (in units of seconds) from when admin-status object of a particular port becomes 'disabled' until reinitialization is attempted.
Maximum Transmit Credits	The maximum number of consecutive LLDPDUs that can be transmitted at any time.
Fast Transmission LLDPDUs count	The default number of LLDPDUs that are transmitted during a fast transmission period.
Fast Transmission Interval	Time interval in timer ticks between transmissions during fast transmission periods.
Chassis ID	The string value used to identify the chassis component associated with the local system.
Chassis ID Subtype	The type of encoding used to identify the chassis associated with the local system.
System Name	The string value used to identify the system name of the local system.
System Description	The string value used to identify the system description of the local system.
System Supported Capabilities	The bitmap value used to identify which system capabilities are supported on the local system. BITS { other(0), repeater(1), bridge(2), accessPoint(3), router(4), telephone(5), wirelessStation(6), stationOnly(7) }
System Enabled Capabilities	The bitmap value used to identify which system capabilities are enabled on the local system. BITS { other(0), repeater(1), bridge(2), accessPoint(3), router(4), telephone(5), wirelessStation(6), stationOnly(7) }
Last Remote Change Time	The value of system-time at the time an entry is created, modified, or deleted
Total Remote Inserts	The number of times the complete set of information advertised by a particular MSAP has been added.
Total Remote Deletes	The number of times the complete set of information advertised by a particular MSAP has been deleted.
Total Remote Drops	The number of times the complete set of information advertised by a particular MSAP could not be processed because of insufficient resources.
Total Remote Ageouts	The number of times the complete set of information advertised by a particular MSAP has been because the information timeliness interval has expired.

The output fields for **lldp traffic interface** include:

Field	Description
Interface	Name of the interface.
RX Frames Discarded	The number of LLDP frames received by this LLDP agent on the indicated port, and then discarded for any reason.
RX Pckts with TLVs Discarded	A count of all LLDPDUs received at the port with one or more detectable errors.
RX Frames Errors	The number of invalid LLDP frames received by this LLDP agent on the indicated port, while this LLDP agent is enabled.
RX Frames Total	The number of valid LLDP frames received by this LLDP agent on the indicated port, while this LLDP agent is enabled.
RX TLVs Discarded	The number of LLDP TLVs discarded for any reason by this LLDP agent on the indicated port.
RX TLVs Errors	The number of LLDP TLVs received on the given ports that are not recognized by this LLDP agent on the indicated port
RX TLVs Total	The counter that represents the number of age-outs that occurred on a given port.

TX Frame Total	The number of LLDP frames transmitted by this LLDP agent on the indicated port
Remote	TBD
Time Mark	TBD

The output fields for **lldp neignbors interface** include:

Local Interface	The index value used to identify the port component (contained in the local chassis with the LLDP agent) associated with this entry. The lldpRemLocalPortNum identifies the port on which the remote system information is received.
Remote Index	The object represents an arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated remote system.
Remote Port	The string value used to identify the port component associated with the remote system.
Port Subtype	The type of port identifier encoding used in the associated. with the remote system.
Chassis Subtype	The type of encoding used to identify the chassis associated with the remote system.
Chassis	The string value used to identify the chassis component associated with the remote system.
MAC Address	Remote MAC address.
System Capability Supported	The bitmap value used to identify which system capabilities are supported on the remote system.
System Capability Enabled	The bitmap value used to identify which system capabilities are enabled on the remote system.
Port Description	The string value used to identify the description of the given port associated with the remote system.
System Name	The string value used to identify the system name of the remote system.
System Description	The string value used to identify the system description of the remote system.
Local Interface	The index value used to identify the port component (contained in the local chassis with the LLDP agent) associated with this entry. The lldpRemLocalPortNum identifies the port on which the remote system information is received.
Address	The string value used to identify the management address component associated with the remote system. The purpose of this address is to contact the management entity.
Address Subtype	monitoring interface to view the remote management addresses as learned from the remote LLDP peer.
Address Interface ID	The integer value used to identify the interface number regarding the management address component associated with the remote system.
Address Interface ID Subtype	The enumeration value that identifies the interface numbering method used for defining the interface number, associated with the remote system.
Address OID	The OID value used to identify the type of hardware component or protocol entity associated with the management address advertised by the remote system agent.

The output fields for **lldp interface**:

Field	Description
Interface	Port's ID.
Port Name	Port's name.
Port Subtype	Port's subtype.

Administrative Status	The administratively desired status of the local LLDP agent.
Port Description	The string value used to identify the system description of the local system.
Port Description Transmit Enable	Capability of LLDP agent to transmit ‘Port Description TLV’.
System Name Transmit Enable	Capability of LLDP agent to transmit ‘System Name TLV’.
System Description Transmit Enable	Capability of LLDP agent to transmit ‘System Description TLV’.
System Capability Transmit Enable	Capability of LLDP agent to transmit ‘System Capabiities TLV’.
Management Address Transmit Enable	Capability of the system management address instance t be transmitted on the ports.
Management Neighbors	Number of remote management addresses (Mgmt. TLVs) detected on the port.
Multiple Neighbors	Enabled if more than one peer has been detected on port.
Port Neighbors	Number of peers detected on the port.
Too Many Neighbors	Enabled if more than 4096 peers have been detected on the port.
Something Changed Local	Internal state representing if something has changed locally, but was still not processed.
Something Changed Remote	Internal state representing if something has changed on remote, but was still not processed.

Revision 1.0.1

Related Commands

show interface (Privileged)

Shows the configuration of all interfaces (ports) or of the specified interface. The output includes port configuration information and port statistics.

Command Syntax

show interface [<*interfaceName*>**] [transceiver]**

show interface [<*interfaceName***>] status errdisable**

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

Command Modes Privileged Mode #

Syntax Description

interfaceName	Name of the interface. For example, **xe1**.
tranceiver	Shows interface status information for the transceiver.
status	Shows interface status information.
errdisable	Shows the ErrDisable status on port.
vlan	Displays information about VLAN interfaces.
vlanId	Specified route interface.

Examples

```
#show interface xe1
#show interface transceiver
#show interface xe1 transceiver
```

```
#show interface status errdisable
#show interface xe1 status errdisable
#show interface vlan
#show interface vlan 1
```

System Response

The output fields for **interface** are as follows:

Field	Description
Port	The system generated, fixed and unique logical port identifier value.
Name	Port name. For example, **xe1**.
Description	Description of the interface.
MAC Address	MAC address of the port.
Type	Physical port type.
Administrative Mode	State of the port.
Operational Status	Operational status of the port.
Auto Negotiate	Port auto-negotiation mode.
Speed	Port speed in kbits/s.
Duplex	Concurrency of the bidirectional communication paths for the interface.
Flow Control	Whether the interface processes received pause frames or sends pause frames.
Maximum Frame Size	Current state of the parameter.
PVID	Port VLAN identifier.
PVPT	Port VLAN priority.
Learning Mode	The method the port uses to learn MAC addresses.
Ingress Filtering	Current state of ingress filtering capability on the port.
Discard Mode	The packet discard mode for the port.
Cut Through	The cut-through interface option allows packets to be transmitted on a port before the entire packet is received.
IGMP Enable	Internet Group Management Protocol (IGMP) mode.

The output fields for **interface transciever** are as follows:

Field	Description
Port	Unique port identifier.
Identifier	Type of transceiver, for example SFP, SFP Plus, XFP, etc.
Type Code	The connector value indicates the external optical or electrical cable connector provided as the media interface.
Compatibility Code	The electronic or optical interfaces that are supported by the transceiver. For example 10G Base-SR
Encoding Code	Serial encoding algorithm code.
Bit Rate	The actual bit rate supported.
Link Length Pairs	Multiple (at least one) pairs of link length and cable types in the form of length/type.
Name	Vendor name.
OUI	Vendor IEEE company id.
Part Number	Vendor part number.
Revision	Vendor revision.
SN	Vendor serial number.
Manufacturing Code	Vendor manufacturing date.
Wavelenght	Laser wavelength, Passive/Active Cable Specs.

Options	Two bytes (raw value) that indicate which transceiver signals options are implemented.
Diagnostic Options	Indicates which type of diagnostics monitoring capabilities implemented (raw code).
Enhanced Options	Enhanced options (raw code).
Compliance 8472	SFF 8472 compliance, i.e. which sub version (raw code).

The output fields for **interface status errdisable** are as follows:

Field	Description
Port Name	Name of the port.
Status Reason	Reason for ErrDisable state.

Revision 1.0.1

Related Commands

interface (modes)
show statistics
show interface (User)

show interface flowcontrol

Shows the flow-control configuration for all interfaces.

Command Syntax **show interface [<*interfaceName*>]flowcontrol**

Command Modes Privileged Mode #

Syntax Description	*interfaceName*	Shows the flow-control configuration for specified interface.

Command Default This command has no default settings.

Examples

```
#show interface flowcontrol
#show interface xe1 flowcontrol
```

System Response The output fields for **port-channel** are as follows:

Field	Description
Interface	The interface for which to show the flow control configuration.
Flow Control	Flow control configuration for the specified interface.

Revision 1.1

Related Commands

flowcontrol

show port-channel

Displays port channel global configuration.

Command Syntax **show port-channel**

Command Modes Privileged Mode #

Syntax Description This command does not have any parameters.

Command Default This command has no default settings.

Examples

```
#show port-channel
```

System Response The output fields for **port-channel** are as follows:

Field	Description
MAC Address	The LAG associated bridge address, taken directly from the current bridge ID.
Priority	The LAG associated bridge priority, which is between 0x0000 to 0xF000 in steps of 0x1000.
Collector Maximum Delay	The maximum time that the frame collector may delay the delivery of a frame received from an aggregator parser to its MAC client, specified in tens of microseconds.
Port Channel Status	Indicates the link aggregation feature status in the system.
Load-balance	The distribution of incoming and outgoing packets amongst the interfaces of a port channel.
Load-balance Mode	The order of ingress or egress packet processing.
LACP Status	Shows whether this port is LACP enabled or not.

Revision 1.0.1

Related Commands

`port-channel load-balance`
`port-channel collector-max-delay`
`port-channel enable`
`no port-channel`

show interface port-channel

Displays link aggregation configuration for administrative interfaces, remote interfaces, or a specific port.

Command Syntax	**show interface port-channel [<*portChannel*>] [{admin | detail | neighbor | status errdisable}]**	
Command Modes	Privileged Mode	#
Syntax Description	*portChannel*	Port channel number. The range is 3800 to 4094.
	admin	Shows port channel administrative configuration.
	detail	Shows port channel detailed configuration.
	neighbor	Shows port-channel neighbor configuration.
	status	Shows interface status information.
	errdisable	Shows the ErrDisable status of the port channel.
Command Default	This command has no default settings.	

Examples

```
#show interface port-channel
#show interface port-channel 3800
#show interface port-channel admin
#show interface port-channel detail
#show interface port-channel neighbor
#show interface port-channel 3800 detail

#show interface port-channel 3800 admin
#show interface port-channel 3800 status errdisable
#show interface port-channel 3800 neighbor
```

System Response

The output fields for **interface port-channel** are as follows:

Field	Description
Port Channel	Port channel number.
Port Channel MAC Address	The LAG associated bridge address, taken directly from the current bridge ID.
Operational Key	The local LAG operational key
Transmit State	Indicates Enabled or Disabled, depending on whether the LAG is transmitting or not.
Receive State	Indicates Enabled or Disabled, depending on whether the LAG is receiving or not.
Ready to Send	Indicates whether the LAG is ready or not.

The output fields for **interface port-channel detail** are as follows:

Field	Description
Port	Port number.
Port Name	Port name.
Description	Port channel description.
Type	Type of the port channel.

Administrative Mode	State of the port.
Operational Status	Operational status of the port.
Learn Mode	The method the port uses to learn MAC addresses: • None—DLFs (destination lookup frames) are not learned, frames are flooded on VLAN. • Hardware—DLFs are learned by hardware, frames are flooded on VLAN. • Software—DLFs are learned by software, frames are flooded on VLAN. • None And Drop—DLFs are not learned, frames are dropped. • Hardware And Drop—DLFs are learned by hardware, frames are dropped. • Software And Drop—DLFs are learned by software, frames are dropped.
Ingress Filtering	When ingress filtering is disabled, the port accepts any VLAN-tagged frame. When ingress filtering is enabled, incoming frames tagged for VLANs which do not include the ingress port are discarded.
Discard Mode	The packet discard mode for the port. None, All, Tagged, or Untagged.
IGMP	Internet Group Management Protocol (IGMP) mode. IGMP snooping listens to IGMP conversations to obtain and maintain a table of links in need of IP multicast streams. Enable or Disable.
PVID	Port VLAN identifier
PVPT	Port VLAN priority
Maximum Frame Size	Max Frame Size as defined by the standard and as it is limited on this hardware.
Port Channel MAC Address	The LAG associated bridge address, taken directly from the current bridge ID.
Operational Key	The local LAG operational key
Transmit State	Indicates Enabled or Disabled, depending on whether the LAG is transmitting or not.
Receive State	Indicates Enabled or Disabled, depending on whether the LAG is receiving or not.
Ready to Send	Indicates whether the LAG is ready or not.
Port Channel Type	Type of the port channel.
Adminitrsative LAG key	The local LAG operational key
Load-balance	The distribution of incoming and outgoing packets amongst the interfaces of a port channel.

The output fields for **interface port-channel admin** are as follows:

Field	Description
Port Channel	Port channel number.
Name	Port name
Port Channel Type	Type of the port channel.
Administrative LAG Key	The local LAG operational key
Load Balance	The distribution of incoming and outgoing packets amongst the interfaces of a port channel.

The output fields for **interface port-channel <*portchannel*> status errdisable** are as follows:

Field	Description
Port Name	Name of the port.
Status Reason	Reason for ErriDisable status.

Revision 1.2

Related Commands

```
port-channel load-balance
port-channel collector-max-delay
port-channel enable
no port-channel
```

show mac-address-table (Privileged)

Shows the forwarding database for the system or for a specific MAC address.

Command Syntax **show mac-address-table [***macAddress***]**

Command Modes Privileged Mode #

Syntax Description *macAddress* MAC address.

Examples

```
#show mac-address-table 00:00:67:00:00:01
#show mac-address-table
```

System Response The output fields for **mac-address-table** are as follows:

Field	Description
Interface	The system generated, fixed and unique logical port identifier value.
MacAddress	MAC address of the port.
Vlan	VLAN identifier
Type	Static or Dynamic
Total MAC addresses count	Number of MAC addresses.
Static MAC addresses count	Number of static MAC addresses.
Dynamic MAC addresses count	Number of dynamic MAC addresses.

Revision 1.0.1

Related Commands

```
mac-address-table
show mac-address-table (User)
```

show mls qos

Shows Multilayer Switching (MLS) Quality of Service (QoS) information.

Command Syntax **show mls qos {bandwidth [interface <***interfaceName***>]|scheduling [interface <***interfaceName***>]|map {dscp-cos|dot1p-cos}}**

Command Modes Privileged Mode #

Syntax Description

bandwidth	Displays MLS QoS bandwidth information for specified interface.
scheduling	Displays MLS QoS scheduling information for specified interface.
interfaceName	Name of an interface port. For example, **xe1**.
map	Displays MLS CoS-to-Dot1p (**dot1p-cos**) or CoS-to-DSCP (**dscp-cos**) mapping information for specified interface.

Examples

```
#show mls qos bandwidth interface xe1
#show mls qos map dot1p-cos
#show mls qos map dscp-cos#show mls qos scheduling interface xe1
```

System Response

The output fields for **mls qos** are as follows:

Field	Description
Port	The system generated, fixed and unique logical port identifier value
Trust Mode	Trust Mode (Untrusted/802.1p/DSCP)
Sched Mode	The scheduling mode.
CoS *n*	The CoS Bandwidth or Schedulings CoS weight allocation as percentage of linerate (0..100) or -1 for no configuration. *n* = 0 to 7.
Dot1p	802.1p priority (0..7)
DSCP	Differentiated Service Code Point.(0..63)

Revision

1.2

Related Commands

`mls qos map (config)`
`wrr-queue bandwidth`
`mls qos map (config-if interface)`
`mls qos trust`

show monitor

Shows interface monitor.

Command Syntax

show monitor

Command Modes

Privileged Mode #

Examples

```
#show monitor
```

System Response

The output fields for **monitor** are as follows:

Field	Description
Mode	Directed or switched.
Preserved mode	Sets global interface preserve monitoring mode.

Source interface	Interface name or interface names list separated by dash or commas that you want to add for mirroring.
Destination interface	Name of the destination interface.
Mode	Mode for egress and ingress packets mirroring.

Revision 1.0.1

Related Commands

show multicast

Shows multicast forwarding information.

Command Syntax **show multicast [static] [<*macAddress*> <*vlanId*>]**

Command Modes Privileged Mode #

Syntax Description

static	Shows static forwarding multicast entries.
vlanId	VLAN to show forwarding multicast information for.
macAddress	MAC address to show forwarding multicast information for.

Examples

```
#vlan-database
(vlan)#vlan 5
(vlan)#exit
#configure
(config)#mac-address-table multicast 01:00:00:00:08:05 vlan
5 interface xe3

#show multicast

VLAN Interface Group MAC Address Group Type
---- --------- ----------------- ----------
5    xe3       01:00:00:00:08:05 Static

#show multicast static 01:00:00:00:08:05 5
```

System Response The output fields for **multicast** are as follows:

Field	Description
Vlan	VLAN Identifier.
Interface	Interface name.
Group MacAddress	AC Address in the format of XY:XX:XX:XX:XX:XX.
Group Type	Describes whether this entry is administrative or dynamically created.

Revision 1.2

Related Commands

`show vlan (User)`
`show vlan (Privileged)`

show ovs

Diplays the current status of the Open-vSwitch configuration.

Command Syntax **show ovs {bridges | ports | {flows [{rule [<*bridgeName*> <*flowId*> <*tableId*>]} | {action [<*bridgeName*> <*flowId*> <*tableId*>]} | {expression [<*bridgeName*> <*flowId*> <*tableId*>]} | {statistics [<*bridgeName*> <*flowId*> <*tableId*>]}]} | resources}**

Command Modes Privileged Mode #

Syntax Description

ovs	Shows open vSwitch configuration.
bridges	Shows OVS bridges.
ports	Shows OVS ports.
flows	Shows OVS flows.
rule	Shows OVS flow rule.
action	Shows OVS flow action.
bridgeName	Bridge name, starts with 'spp' following by bridge-id (e.g. - 'spp0').
flowId	Specify flow id.
tableId	Flow table id to specify.
expression	Shows OVS flow expression.
statistics	Shows OVS flow statistics.
resources	Shows OVS resources.

Command Default This command has no default settings.

Examples

```
#show ovs bridges
#show ovs flows
#show ovs ports
#show ovs resources
#show ovs flows spp0 1 1
```

System Response The output fields are as follows:

Field	Description
Bridge	Bridge identifier
Name	Bridge name starts with 'spp' following by bridge-id (e.g.'spp0').
Type	Type of the bridge.
Controller	OpenFlow controller end-point.
Rules Limit	Open-vSwitch rules limit. The range is from 0 to 4096.
Table	Flow table identifier.
Priority	OpenFlow flow priority.

Qualifiers	Ovs-ofctl qualifier.
Actions	Ovs-ofctl action.
Duration	Amount of time the flow has been installed in the switch
Total Bytes	Number of received packets per flow.
Total Packets	Number of received bytes per flow.
Port	Port number.
VLANs Limit	The OVS VLANs limit. The \a vlansLimit defines the number of VLANs created for OVS usage. When OVS bridge is created, VLANs 1-'vlansLimit' are created, and each OVS port is associated with all of these VLANs. NOTE: This value can only be changed before OVS bridges are created.
Untagged VLAN	The OVS untagged-VLAN. The VLAN which is used for untagged frames switching. This VLAN will also be used as the default VLAN (PVID) on all OVS ports. NOTE: This value can only be changed before OVS bridges are created.

Revision 1.2

Related Commands

`ovs bridge add`
`ovs bridge controller`
`ovs flow add`
`ovs resources rules-limit`
`ovs resources vlans-limit`
`ovs resources untagged-vlan`

show spanning-tree

Shows the global spanning-tree configuration.

Command Syntax **show spanning-tree**

Command Modes Privileged Mode #

Command Default This command has no default settings.

Examples

```
#show spanning-tree
```

System Response The output fields are as follows:

Field	Description
Aging Time	Aging Time can be from 10 to 1,000,000 seconds
Bridge ID	The bridge’s MAC address
Bridge Priority	Bridge priority
CIST Root Path Cost	The CIST path cost from the transmitting bridge to the CIST Regional Root.
Designated Root	The designated root bridge MAC address
Force Version	Forced Version, needs to be 0 to force STP and 2 for RSTP, 3 for MSTP.
Forward Delay	Bridge Forward Delay Time
Global Enable	Enable or disable STP for this bridge
Hello Time	Bridge Hello Time

Maximum Age	Bridge Max Age Time
Maximum Hops	Defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region.
Migration Time	Port Migration Time
Mode	Set the STP mode to STP, RSTP, or MSTP, which can be only one mode per bridge.
Root Path Cost	Root Path Cost to the Root Bridge (For MSTP this is the CIST External Root Path Cost).
Root Port ID	The designated root port identifier
Root Times Forward Delay	Root times structure component - Forward Delay
Root Times Hello Time	
Root Times Maximum Age	Root times structure component - Max Age
TC	Asserted if the tcWhile timer for any port is non-zero.
TC Count	The count of times that there has been at least one non-zero tcWhile timer.
Time Since TC	The count in seconds of the time since the tcWhile timer for any port was nonzero.
TX Hold Count	Protocol transmit hold count in seconds Hold Time, equal to the number of hops to hold.

Revision 1.0.1

Related Commands

```
spanning-tree
spanning-tree mst configuration
show spanning-tree mst
show spanning-tree interface
```

show spanning-tree interface

Shows the spanning-tree configuration for all ports or a specific interface port or per port-channel.

Command Syntax **show spanning-tree interface [<***interfaceName***> | {port-channel <***portChannel***>}]**

Command Modes Privileged Mode #

Syntax Description

interface	Displays STP information for all interfaces.
interfaceName	Name of the interface. For example **xe1**.
port-channel	Display STP information per port channel.
portChannel	Port channel number. The range is 3800 to 4094.

Command Default This command has no default settings.

Examples

```
#show spanning-tree interface
#show spanning-tree interface xe1
#show spanning-tree interface port-channel 3800
```

System Response The output fields for **spanning-tree interface** are as follows:

Field	Description
Interface	The system generated, fixed and unique logical port identifier value and the second of two primary keys for this table.

Administrative Edge Port	Identifies if adminEdgePort is set for an interface.
Administrative Point To Point MAC	Specifies whether the port behave as a point2point MAC.
Administrative State	Identifies whether this port participates in STP.
Auto Edge Port	Specifies whether automatic discovery of Edge ports is enabled.
Cost	Port cost calculated based on the port's speed taken from the Ports table.
Designated Bridge	The unique Bridge Identifier of the Bridge to which the Port belongs, in the case of a Designated Port; or otherwise, the Bridge believed to be the Designated Bridge for the LAN to which this Port is attached.
Designated Cost	For a Designated Port, the path cost offered to the LAN to which the Port is attached; otherwise, the cost of the path to the Root offered by the Designated Port on the LAN to which this Port is attached.
Designated Port	The Port Identifier of the Bridge Port, on the Designated Bridge, through which the Designated Bridge transmits the Configuration Message information stored by this Port.
Designated Root	The unique Bridge Identifier of the Root Bridge.
Enabled	Indicates the specified port is enabled for STP operation (ONS parameter, not protocol defined).
MAC Enabled	The current state of the MAC Enabled parameter.
MAC Operational	The current state of the MAC Operational parameter.
Mcheck Status	Current status of mcheck.
Operational Edge Port	Specifies whether the port is an Edge port or not.
Operational Point To Point MAC	Current state of the operPointToPointMAC parameter.
Port Transition	Bit field to show the state of PPSSAA: Proposing, Proposed, Sync, Synced, Agree, Agreed
Priority	The port priority, from 0 to 240 in incriments of 16.
Role	The port’s role.
RX Config BPDU Counter	Counts the number of received BPDUs from the enable time of this port (ONS parameter, not protocol defined).
RX Rstp BPDU Counter	Counts the number of received RSTP BPDUs from the enable time of this port (ONS parameter, not protocol defined).
RX TC BPDU Counter	Counts the number of received TC BPDUs from the enable time of this port (ONS parameter, not protocol defined).
RX TCN BPDU Counter	Counts the number of received TCN BPDUs from the enable time of this port (ONS parameter, not protocol defined).
State	Current port state.
TC Ack	Specifies if a configuration message with a topology change acknowledge flag set was transmitted.
RX Config BPDU Counter	Counts the number of sent BPDUs from the enable time of this port (ONS parameter, not protocol defined).
RX Rstp BPDU Counter	Counts the number of sent RSTP BPDUs from the enable time of this port (ONS parameter, not protocol defined).
RX TC BPDU Counter	Counts the number of sent TC BPDUs from the enable time of this port (ONS parameter, not protocol defined).
RX TCN BPDU Counter	Counts the number of sent TCN BPDUs from the enable time of this port (ONS parameter, not protocol defined).
Uptime	Count in seconds of the time elapsed since the Port was last reset or initialized.

Revision 1.0.1

Related Commands

show spanning-tree
spanning-tree mst configuration
show spanning-tree mst

```
show spanning-tree interface
```

show spanning-tree mst

Shows the spanning-tree configuration for all multiple spanning trees (MSTs) or for a specific interface.

Command Syntax	**show spanning-tree mst configuration | <***mstRegion***> | interface [<***interfaceName***>|port-channel <***portChannel***>]**	
Command Modes	Privileged Mode	#
Syntax Description	**configuration**	Display the MST region configuration.
	interface	Display MST information for instances.
	interfaceName	Name of an interface port. For example, **xe1.**
	port-channel	Display the STP information per port-channel.
	portChannel	Number of a port-channel.
	mstRegion	Display the MST region for the specified instance.
Command Default	This command has no default settings.	

Examples

```
#show spanning-tree mst configuration
#show spanning-tree mst 8
#show spanning-tree mst interface port-channel 3800
#show spanning-tree mst interface
#show spanning-tree mst interface xe1
```

System Response

The output fields for **spanning-tree mst configuration** are as follows:

Field	Description
Name	Name of MST configuration
Revision Level	MST Configuration revision level
Digest Signature Key	The Configuration Digest is a 16-octet signature of type HMAC-MD5 (see IETF RFC 2104) created from the MST Configuration table.
Format Selector	The value is set to 0.
MSTI	MSTP Instance ID.
VLANs Mapped	VLANs mapped to MST Instance.

Field	Description
MST Instance	MST instance identifier
Bridge ID	The bridge identifier for the spanning tree instance identified by the MSTID
Bridge Priority	Bridge priority
Bridge Forward Delay	Bridge Forward Delay time
Bridge Hello Time	Bridge Hello time
Bridge Maximum Age	Bridge Max Age time
Designated Root	The designated root bridge MAC address
Root Port ID	The designated root port identifier
Root Path Cost	The root path cost
Root Priority	Designated root Bridge Priority.
Root Forward Delay	Root Forward Delay value.

Root Maximum Age	Root Max Age value.
TC	True if tcWhile is non-zero for any port for the given MST (tcWhile).
TC Count	The count of the times tcWhile has been non-zero for any Port for the given MSTI since the bridge was powered on or initialized.
Time Since TC	The count in seconds of the time elapsed since tcWhile was last non-zero for any port for the given MSTI.
TX Limit	Maximum number of MST BPDUs transmitted per second.
MST Port Configuration Table	A list of Port Ids, in this tree based on their VLAN associations.
VLANs	Range of VLANs for the specified instance.
Interface	Name of an interface.
Role	Role of the port.
State	State of the port.
Internal Cost	Cost back to the Regional Root.
External Cost	External path cost for the port.
Priority	The port priority, from 0x0000 to 0x00F0 in steps of 0x0010
Type	Type of the port.

The output fields for **spanning-tree mst interface** are as follows:

Field	Description
Interface	The system generated, fixed and unique logical port identifier value and the second of two primary keys for this table.
MST Instances	Unique MST instance identifier
Administrative Point To Point MAC	Specifies whether the port behave as a point2point MAC
Administrative State	Specifies whether this port participates in STP
Administrative Edge Port	Specifies if this port behaves as an Edge port
Designated Bridge	Unique Bridge Identifier of the Bridge to which the Port belongs, in the case of a Designated Port; or otherwise, the Bridge believed to be the Designated Bridge for the LAN to which this Port is attached.
Designated Cost	For a Designated Port, the path cost offered to the LAN to which the Port is attached; otherwise, the cost of the path to the Root offered by the Designated Port on the LAN to which this Port is attached.
Designated Port	For a Designated Port, the path cost offered to the LAN to which the Port is attached; otherwise, the cost of the path to the Root offered by the Designated Port on the LAN to which this Port is attached.
Designated Root	Unique Bridge Identifier of the Root Bridge
Disputed	Current value of the disputed variable for the CIST for the Port (13.24, and 17.19 of IEEE Standard 802.1D)
Enabled	Indicates the specified port is enabled for MSTP operation (ONS parameter, not protocol defined)
External Cost	External path cost for the port
Internal Cost	Cost back to the Regional Root
MAC Enabled	Current state of the MAC Enabled parameter
MAC Operational	Current state of the MAC Operational parameter
Mcheck Status	Current status of mcheck
Operational Edge Port	Specifies whether the port is an Edge port or not
Operational Point To Point MAC	Current state of the operPointToPointMAC parameter
Port Hello Time	Port Hello Time

Port Transition	Bit field to show the state of PPSSAA: Proposing, Proposed, Sync, Synced, Agree, Agreed
Priority	Maximum number of MST BPDUs transmitted per second.
Restricted Role	The current state of the parameter for the port
Restricted Tcn	The current state of the parameter for the port
Role	Role of the port
State	State of the port
TC Ack	Maximum number of MST BPDUs transmitted per second.
Uptime	Count in seconds of the time elapsed since the Port was last reset or initialized.
RX Config BPDU Counter	Counts the number of received BPDUs from the enable time of this port (ONS parameter, not protocol defined).
RX MSTP BPDU Counter	Counts the number of received MSTP BPDUs from the enable time of this port (ONS parameter, not protocol defined).
RX RSTP BPDU Counter	Counts the number of received RSTP BPDUs from the enable time of this port (ONS parameter, not protocol defined).
RX TC BPDU Counter	Counts the number of received TC BPDUs from the enable time of this port (ONS parameter, not protocol defined).
RX TCN BPDU Counter	Counts the number of received TCN BPDUs from the enable time of this port (ONS parameter, not protocol defined).
TX Config BPDU Counter	Counts the number of sent BPDUs from the enable time of this port (ONS parameter, not protocol defined).
TX MSTP BPDU Counter	Counts the number of sent MSTP BPDUs from the enable time of this port (ONS parameter, not protocol defined).
TX RSTP BPDU Counter	Counts the number of sent RSTP BPDUs from the enable time of this port (ONS parameter, not protocol defined).
TX TC BPDU Counter	Counts the number of sent TC BPDUs from the enable time of this port (ONS parameter, not protocol defined).
TX TCN BPDU Counter	Counts the number of sent TCN BPDUs from the enable time of this port (ONS parameter, not protocol defined).

Revision 1.0.1

Related Commands

show system

Shows the configuration of the system hardware and software.

Command Syntax **show system**

Command Modes Privileged Mode #

Examples

```
#show system
```

System Response The output fields for **system** are as follows:

Field	Description
Name	Platform name
Ethernet Switch Type	Platform hardware
Model	Platform model number
Platform	Platform hardware name

Chip Version	Ethernet Chip version
Chip Subtype	Ethernet Chip sub type
API Version	Ethernet Chip API version
Software Version	ONS version
CPU	Platform CPU type
CPU Architecture	Platform CPU architecture
OS	Platform OS type
OS Version	Platform OS version
Serial Number	Platform serial number
IP Address	System IP address
Mask	System network mask
Gateway	System gateway
MAC Address	System MAC address

Revision 1.0.1

Related Commands

```
show running-config
show version
```

show statistics

Shows the statistics for all ports or for a specific port.

Command Syntax **show statistics interface [<***InterfaceName***> | cpu]**

Command Modes Privileged Mode #

Syntax Description

interfaceName	Name of an interface port. For example, **xe1**.
cpu	Shows CPU interface statistoics information

Command Default This command has no default settings.

Examples

```
#show statistics interface xe1
#show statistics interface cpu
```

System Response The output fields for **statistics** are as follows:

Field	Description
Port	Port identifier
Name	Name of the port interface
RX Broadcast Pkts	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. (RFC 1573)
RX Discards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to higher-layer protocol. (RFC 1213)
RX Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher layer

	protocol. (RFC 1213)
RX Multicast Pkts	The number of packets, delivered by this sub-layer to a higher (sub-) layer, which were addressed to a multicast address at this sub-layer. (RFC 1573)
RX NUcast Pkts	The number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher layer protocol. (RFC 1213)
RX Octecs	The total number of octets received on the interface, including framing characters. (RFC 1213)
RX Ucast Pkt	The number of subnetwork-unicast packets delivered to a higher-layer protocol. (RFC 1213)
TX Broadcast Pkts	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. (RFC 1573)
TX Discards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. (RFC 1213)
TX Errors	The number of outbound packets that could not be transmitted because of errors. (RFC 1213)
TX Multicast Pkts	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. (RFC 1573)
TX NUcast Pkts	The total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent. (RFC 1213)
TX Octets	The total number of octets transmitted out of the interface, including framing characters. (RFC 1213)
TX QLen	The length of the output packet queue (in packets). (RFC 1213)
TX Ucast Pkts	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent. (RFC 1213)

Revision 1.0.1

Related Commands

`clear statistics`
`clear config`
`show interface`
`show statistics`

show storm-control

Shows the configuration of the storm control parameters.

Command Syntax **show storm-control**

Command Modes Privileged Mode #

Examples

```
#show storm-control
```

System Response The output fields for **storm-control** are as follows:

Field	Description

Port	The system generated, fixed and unique logical port identifier value.
Stage	The storm control port stage.
Frame type	The storm control frame type.
Capacity [Bytes]	The buffer capacity limit for storing queued packets; meaning, the maximum buffer allocation for classified packets
Rate [Kbit/s]	The maximum average rate limit for classified packets, specify in kbps.

Revision 1.0.1

Related Commands

`flowcontrol`

show running-config

Shows the current configuration of the system and all port interfaces. The output includes:

- VLAN database
- Switch configuration
- VLAN configuration
- 802.1Q configuration
- MLS QOS configuration
- Spanning tree configuration
- IGMP configuration
- LLDP configuration
- OVS configuration
- Interface port configuration (all ports)
- Interface VLAN configuration
- ARP configuration
- Router OSPF configuration

Command Syntax **show running-config [interface <***interfaceRange***> | mgmt-ethernet | port-channel <***portChannelRange***>]**

Command Modes Privileged Mode #

Syntax Description

interface	Shows running configuration for specified interface.
interfaceRange	Interface name or interfaces list to show information for.
mgmt-ethernet	Shows running config information for a management port.
port-channel	Shows running configuration for specified port channel.
portChannelRange	Port channel name or port channels list to show information for.

Examples

```
Switch #show running-config

enable

 vlan-database

  vlan 1,10,2

 exit

 configure

  switch mac-address 00:01:10:00:03:01
  switch default-vlan 1
  switch aging-time 300

  ip address 2.2.2.2 255.255.255.0

  vlan 1
   name "Default VLAN"
  exit

  vlan 10
   name "VLAN-10"
  exit
```

Revision 1.0.1

Related Commands

`show tech-support`
`show version`
`show system`

show tech-support

Shows the configuration of all interfaces and of the ONP switch.

Command Syntax **show tech-support**

Command Modes Privileged Mode #

Examples

```
#show tech-support
```

Revision 1.0.1

Related Commands

`show system`
`show running-config`
`show version`

show terminal

Shows terminal session configuration.

Command Syntax **show terminal**

Command Modes Privileged Mode #

Command Default Default terminal length is 24.

Examples

```
#show terminal
```

System Response The output fields for **show terminal** are as follows:

Field	Description
Terminal Length	Number of lines used to paginate command output.

Revision 1.1

Related Commands

`terminal length (User)`
`terminal length (Privileged)`
`show terminal (User)`

show ufd

Shows UFD feature configuration information.

Command Syntax	**show ufd [groups [<*groupId*>]**	
Command Modes	Privileged Mode	#
	ufd	Shows UFD feature configuration information.
	groups	Shows UFD groups information.
	groupId	Unique group ID number to show information for. If *groupId* is not entered, the information about all configured groups is displayed.

Examples

```
#show ufd
#show ufd groups
#show ufd groups 1

Switch >enable
Switch #show ufd

Global UFD feature state ................ Enabled
Recovery delay time ..................... 3

Switch #show ufd groups

Group ................................... 100
Threshold ............................... 2
Enable .................................. Enabled
Active Ports ............................ 0
Counter ................................. 1
Failure Action .......................... Active

Group interfaces:

Interface Type       Status
--------- ---------- ---------------
10        LtM        UfdDown
11        LtM        UfdDown
12        LtD        UfdDown

Group ................................... 200
Threshold ............................... 1
Enable .................................. Disabled
Active Ports ............................ 0
Counter ................................. 0
Failure Action .......................... Disabled

Group interfaces:

Interface Type       Status
--------- ---------- ---------------
20        LtM        UfdDown
21        LtD        UfdDown
```

Command Default

System Response

The output fields for **show ufd** are as follows:

Field	Description
Global UFD feature state	Enable or Disable the UFD feature
Recovery delay time	Minimum time that is needed for bring up ports in downlink group.

The output fields for **show ufd groups** are as follows:

Field	Description
Group	The unique id of the group.
Threshold	Minimum number of uplink ports that should be active to hold the downlink group in UfdUp status.
Enable	Enable or Disable UFD group.
Active Ports	Number of monitored ports that are active.
Counter	Counter of link failure detection.
Failure Action	Status of uplink failure detection: Inactive - The uplink or uplinks are up. Active - The switch has detected an uplink failure and has brought the downlink down. Disabled - The switch has disabled UFD per group or switch.
Interface	Port ID.
Type	Type of UFD port: LtM - link to monitor. LtD - link to disable.
Status	UFD port status.

The output fields for **show groups 1** are as follows:

Field	Description
Group	The unique id of the group.
Threshold	Minimum number of uplink ports that should be active to hold the downlink group in UfdUp status.
Enable	Enable or Disable UFD group.
Active Ports	Number of monitored ports that are active.
Counter	Counter of link failure detection.
Failure Action	Status of uplink failure detection: Inactive - The uplink or uplinks are up. Active - The switch has detected an uplink failure and has brought the downlink down. Disabled - The switch has disabled UFD per group or switch.
Interface	Port ID.
Type	Type of UFD port: LtM - link to monitor. LtD - link to disable.
Status	UFD port status.

Revision 1.2

Related Commands

show users

Shows information about currently logged in users.

Command Syntax **show users**

Command Modes Privileged Mode #

Examples

```
>show users
onsadmin console       Jan  1 20:36
admin    pts/1         Jan  2 15:24 (128.224.22.179)
```

Revision 1.0.1

Related Commands

show vlan (Privileged)

Shows the VLAN configuration for all VLANs or for a specific VLAN.

Command Syntax **show vlan [*vlanId*]**

Command Modes Privileged Mode #

Examples

```
#show vlan 1
#show vlan
```

System Response The output fields for **vlan** are as follows:

Field	Description
Name	VLAN name
Port	The system generated, fixed and unique logical port identifier value.
Tagged	Tagged or Untagged designation
Vlan	The system generated, fixed and unique VLAN identifier value.

Revision 1.0.1

Related Commands

interface (modes)
switchport (config-if interface)
vlan-database (mode)
wrr-queue
show vlan (User)

terminal length

This command configures the terminal length.

Command Syntax **[no] terminal length <*terminalLength*>**

Command Modes	Privileged Mode	#
Syntax Description	*terminalLength*	New value for terminal length.

Command Default Default value for [no] command is 24.
0 - sets unlimited terminal length.

Examples

```
#terminal length 1
#no terminal length
```

System Response The output fields for **terminal length** are as follows:

Field	Description
Terminal Length	Number of lines used to paginate command output.

Revision 1.1

Related Commands

`terminal length (User)`
`show terminal (User)`
`show terminal (Privileged)`

6.3 Global Configuration Mode Commands

Use the **configure** command from the Privileged mode (#) to access the Global Configuration mode (config). The Global Configuration mode allows you to configure port and system parameters.

access-list action

Configures extended access list entry.

Note: Rules are defined in the ACLRules table. This table associates a unique Rule ID with an Action ID. Action is previously defined in ACLActions table. A Rule ID can be associated only with a single Action ID. Only one Action can be created for a specific ID.

Command Syntax

access-list action <*aclActionId*> **{permit | deny | normal | {redirect {**<*interfacesRange*> **|** <*portChannel*>**}} | flood | copy-to-cpu | trap-to-cpu | {mirror {ingress | egress}** <*port*>**} | count | {forward- to-tunnel** <*tunnelId*>**} | {set {{vlan {{inner | outer} {**<*setVlanId*> **| {priority** <*setVlanPriority*>**}}}}| {tos** <*tos*>**}| {cos** <*cos*>**}| {policer <policerId>}| {tunnel** <*tunnelId*>**}| {flood-destination interface {**<*interfaceName*> **| {port-channel** <*portChannelId*>**}}}}}}**

no access-list action <*aclActionId*>

Command Modes Configuration Mode `(config)#`

Syntax Description

access-list	Adds an access list entry.
action	Configures extended access list entry.
aclActionId	Access list number.
permit	Permits access if the conditions match.
deny	Denies access if the conditions match.
normal	Redirects packet normally.
redirect	Redirects packet to the listed ports.
interfacesRange	Interfaces on which packets to be redirected.
portChannel	Port-channels on which packets to be redirected.
flood	Floods packets on all ports.
copy-to-cpu	Sends copy of the packet to CPU.
trap-to-cpu	Redirects packet to CPU.
mirror	Mirrors this packet.
ingress	Mirrors this packet upon ingress.
egress	Mirrors this packet upon egress.
port	Destination interface.
count	Increments ACL counter.

set	Sets packet field.
vlan	Sets vlan.
inner	Sets inner VLAN ID.
outer	Sets outer VLAN ID.
vlanId	VLAN ID to be set.
priority	Sets VLAN priority.
vlanPriority	Specifies VLAN priority to be set.
tos	Sets ToS
tos	ToS to be set.
cos	Sets CoS.
cos	CoS to set.
policer	Sets ACL policer ID.
policerId	ACL policer ID to be set.
tunnel	Sets source tunnel ID.
tunnelId	Source tunnel ID to be set.
flood-destination interface	Sets interface to which traffic is to be flooded.
interfaceName	Interface name.
port-channel	Interface port channel to which traffic is to be flooded.
portChannelId	Interface port channel.

Command Default

Examples

```
(config)#access-list action 1 permit
(config)#access-list action 1 deny
(config)#access-list action 1 normal
(config)#access-list action 1 redirect xe1-xe2
(config)#access-list action 1 redirect 3800
(config)#access-list action 1 flood
(config)#access-list action 1 copy-to-cpu
(config)#access-list action 1 mirror ingress xe1
(config)#access-list action 1 mirror egress xe1
(config)#access-list action 1 count
(config)#access-list action 1 set vlan inner priority 1
(config)#access-list action 1 set vlan outer priority 1
(config)#access-list action 1 set tos 1
(config)#access-list action 1 set cos 1
(config)#access-list action 1 set policer 1
(config)#access-list action 1 set tunnel 1
(config)#access-list action 1 set flood-destination
```

```
interface xe1
(config)#access-list action 1 set flood-destination
interface port-channel 3800
(config)#no access-list action 1
```

Revision 1.2

Related Commands

access-list arp ip

Configures the permit or deny clauses to forward or drop ARP packets based on sender IP address.

Command Syntax **access-list standard <***accessListNumber***> permit|deny arp ip any|{host <***senderIp***> <***senderIpMask***> any}| {host <***targetIp***> <***targetIpMask***> {mac any|{host <***senderMac***> <***senderMacMask***> any| host <***targetMac***> <***targetMacMask***>**

Command Modes Configuration Mode `(config)#`

Syntax Description

standard	Configures standard access list entry.
accessListNumber	Access list number. Valid range for access list numbers is 1-16777216. .
permit	Specifies to apply QoS to the flows.
deny	Skips the QoS action that is configured for traffic matching this ACE.
arp ip	Specifies the IP ARP packets.
any	Specifies any IP ARP packets.
host	Specifies a single sender host.
senderIp	IP address of the host sender.
senderIpMask	Mask of the host sender.
any	Specify any target address.
host	Specify a single target host.
targetIp	IP address of the target host.
targetIpMask	Mask of the target host.
mac	Specifies the sender MAC address.
any	Specifies any sender MAC address.
host	Specifies a single sender host MAC address.

senderMac	MAC address of the host sender.
senderMacMask	Mask of the host sender.
any	Specifies any target address.
host	Specifies a single target host MAC address.
targetMac	MAC address of the target host.
targetMacMask	Mask of the target host.

Command Default

Examples

```
(config)#access-list standard 500 deny arp ip any any mac
any any
(config)#access-list standard 100 permit arp ip host 1.1.1.1
255.255.255.0 host 2.2.2.2 255.255.255.0 mac host
f2:0d:db:d8:6c:4c ff:ff:ff:ff:ff:ff host f2:0d:db:d8:6c:4c
ff:ff:ff:ff:ff:ff
```

Revision 1.2

Related Commands

`show access-lists`
`show access-groups`

access-list arp request ip

Configures the permit or deny clauses to forward or drop ARP packets based on ARP requests.

Command Syntax **access-list** <*accessListNumber*> **permit|deny arp request ip any|host <***senderIp***> <***senderIpMask***> any|host <***targetIp***> <***targetIpMask***> mac any|host <***senderMac***> <***senderMacMask***> any|host <***targetMac***> <***targetMacMask***>**

Command Modes Configuration Mode `(config)#`

Syntax Description

accessListNumber	Access list number. Valid range for access list numbers is 1-16777216. .
permit	Specifies to apply QoS to the flows.
deny	Skips the QoS action that is configured for traffic matching this ACE.
arp ip	Specifies the IP ARP packets.
any	Specifies any IP ARP packets.
host	Specifies a single sender host.
senderIp	IP address of the host sender.
senderIpMask	Mask of the host sender.

any	Specify any target address.
host	Specify a single target host.
targetIp	IP address of the target host.
targetIpMask	Mask of the target host.
mac	Specifies the sender MAC address.
any	Specifies any sender MAC address.
host	Specifies a single sender host MAC address.
senderMac	MAC address of the host sender.
senderMacMask	Mask of the host sender.
any	Specifies any target address.
host	Specifies a single target host MAC address.
targetMac	MAC address of the target host.
targetMacMask	Mask of the target host.

Command Default

Examples

```
 (config)#access-list 100 permit arp request ip host 1.1.1.1
255.255.255.0 host 2.2.2.2 255.255.255.0 mac host
f2:0d:db:d8:6c:4c ff:ff:ff:ff:ff:ff host f2:0d:db:d8:6c:4c
ff:ff:ff:ff:ff:ff
```

Revision 1.0.1

Related Commands

`show access-lists`
`show access-groups`

access-list arp response ip

Configures the permit or deny clauses to forward or drop ARP packets based on ARP responses.

Command Syntax **access-list <***accessListNumber***> permit|deny arp response ip any|{host <***senderIp***> <***senderIpMask***> any}| {host <***targetIp***> <***targetIpMask***> {mac any|{host <***senderMac***> <***senderMacMask***> any| host <***targetMac***> <***targetMacMask***>**

Command Modes Configuration Mode `(config)#`

Syntax Description

accessListNumber	Access list number. Valid range for access list numbers is 1-16777216. .

permit	Specifies to apply QoS to the flows.
deny	Skips the QoS action that is configured for traffic matching this ACE.
arp ip	Specifies the IP ARP packets.
any	Specifies any IP ARP packets.
host	Specifies a single sender host.
senderIp	IP address of the host sender.
senderIpMask	Mask of the host sender.
any	Specify any target address.
host	Specify a single target host.
targetIp	IP address of the target host.
targetIpMask	Mask of the target host.
mac	Specifies the sender MAC address.
any	Specifies any sender MAC address.
host	Specifies a single sender host MAC address.
senderMac	MAC address of the host sender.
senderMacMask	Mask of the host sender.
any	Specifies any target address.
host	Specifies a single target host MAC address.
targetMac	MAC address of the target host.
targetMacMask	Mask of the target host.

Command Default

Examples

```
(config)#access-list 500 deny arp response ip any any mac
any any
(config)#access-list 100 permit arp response ip host 1.1.1.1
255.255.255.0 host 2.2.2.2 255.255.255.0 mac host
f2:0d:db:d8:6c:4c ff:ff:ff:ff:ff:ff host f2:0d:db:d8:6c:4c
ff:ff:ff:ff:ff:ff
```

Revision 1.0.1

Related Commands

`show access-lists`
`show access-groups`

access-list expression

Configures access list expression entries.

Note: Rules are defined in the ACLRules table. This table associates a unique Rule ID with an Expression ID. Expression is previously defined in ACLExpressions table. A Rule ID can be associated only with a single Expression ID. Only one Expression can be created for a specific ID.

Command Syntax

access-list expression <*aclExpressionId*> **mac {{source** <*srcMac*> **[**<*srcMacMask*>**] [destination** <*dstMac*> **[**<*dstMacMask*>**]]} | {destination** <*dstMac*> **[**<*dstMacMask*>**]}} [vlan {{ outer {{** <*outerVlan*> **[priority** <*outerVlanPriority*> **] [cfi** <*outerVlanCfi*> **] } | { priority** <*outerVlanPriority*> **[cfi** <*outerVlanCfi*> **] } | { cfi** <*outerVlanCfi*> **}} [inner {{** <*innerVlan*> **[priority** <*innerVlanPriority*> **] [cfi** <*innerVlanCfi*> **] } | { priority** <*innerVlanPriority*> **[cfi** <*innerVlanCfi*> **] } | { cfi** <*innerVlanCfi*> **}}] [format {untagged | tagged}] } | { inner {{** <*innerVlan*> **[priority** <*innerVlanPriority*> **] [cfi** <*innerVlanCfi*> **] } | { priority** <*innerVlanPriority*> **[cfi** <*innerVlanCfi*> **] } | { cfi** <*innerVlanCfi*> **}} [format {untagged | tagged}] } | { format {untagged | tagged} }}] [ethertype** <*ethtype*>**] [ip {{ source** <*srcIp*> <*srcIpMask*> **[destination** <*dstIp*> <*dstIpMask*> **] [protocol {**<*protocolDecVal*> **| {hopopt | icmp | igmp | ggp | ipv4 | st | tcp | cbt | egp | igp | bbn-rcc-mon | nvp-ii | pup | xnet | udp | dcn-meas | hmp | prm | rdp | irtp | iso-tp4 | netblt | mfe-nsp | merit-inp | dccp | 3pc | idpr | xtp | ddp | idpr-cmtp | tp++ | il | ipv6 | sdrp | ipv6-route | ipv6-frag | idrp | rsvp | gre | mhrp | esp | ah | i-nlsp | narp | tlsp | skip | ipv6-icmp | ipv6-nonxt | ipv6-opts | rvd | ippc | sat-mon | visa | ipcv | cpnx | cphb | wsn | pvp | br-sat-mon | vmtp | secure-vmtp | iptm | dgp | ospf | sprite-rpc | larp | mtp | ipip | micp | scc-sp | etherip | encap | ifmp | pim | aris | scps | ipcomp | snp | compaq-peer | vrrp | pgm | l2tp | ddx | iatp | stp | srp | smp | pipe | sctp | fc}}] [type {ipv4-any | ipv6-any | non-ip | {arp {request | reply}}}] [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size** <*ipHeaderSize*> **] } | { destination** <*dstIp*> <*dstIpMask*> **[protocol {**<*protocolDecVal*> **| {hopopt | icmp | igmp | ggp | ipv4 | st | tcp | cbt | egp | igp | bbn-rcc-mon | nvp-ii | pup | xnet | udp | dcn-meas | hmp | prm | rdp | irtp | iso-tp4 | netblt | mfe-nsp | merit-inp | dccp | 3pc | idpr | xtp | ddp | idpr-cmtp | tp++ | il | ipv6 | sdrp | ipv6-route | ipv6-frag | idrp | rsvp | gre | mhrp | esp | ah | i-nlsp | narp | tlsp | skip | ipv6-icmp | ipv6-nonxt | ipv6-opts | rvd | ippc | sat-mon | visa | ipcv | cpnx | cphb | wsn | pvp | br-sat-mon | vmtp | secure-vmtp | iptm | dgp | ospf | sprite-rpc | larp | mtp | ipip | micp | scc-sp | etherip | encap | ifmp | pim | aris | scps | ipcomp | snp | compaq-peer | vrrp | pgm | l2tp | ddx | iatp | stp | srp | smp | pipe | sctp | fc}}] [type {ipv4-any | ipv6-any | non-ip | {arp {request | reply}}}] [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size** <*ipHeaderSize*> **] } | { protocol {**<*protocolDecVal*> **| {hopopt | icmp | igmp | ggp | ipv4 | st | tcp | cbt | egp | igp | bbn-rcc-mon | nvp-ii | pup | xnet | udp | dcn-meas | hmp | prm | rdp | irtp | iso-tp4 | netblt | mfe-nsp | merit-inp | dccp | 3pc | idpr | xtp | ddp | idpr-cmtp | tp++ | il | ipv6 | sdrp | ipv6-route | ipv6-frag | idrp | rsvp | gre | mhrp | esp | ah | i-nlsp | narp | tlsp | skip | ipv6-icmp | ipv6-nonxt | ipv6-opts | rvd | ippc | sat-mon | visa | ipcv | cpnx | cphb | wsn | pvp | br-sat-mon | vmtp | secure-vmtp | iptm | dgp | ospf | sprite-rpc | larp | mtp | ipip | micp | scc-sp | etherip | encap | ifmp | pim | aris | scps | ipcomp | snp | compaq-peer | vrrp | pgm | l2tp | ddx | iatp | stp | srp | smp | pipe | sctp | fc}} [type {ipv4-any | ipv6-any | non-ip | {arp {request | reply}}}] [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size** <*ipHeaderSize*> **] } | { type {ipv4-any | ipv6-any | non-ip | {arp**

{request | reply}}} [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { flags {df | mf} [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { fragment {no-frag | no-frag-or-head | head | sub | any} [header-size <*ipHeaderSize*>] } | { header-size <*ipHeaderSize*> }}] [ipv6 {{ source <*srcIpv6Prefix*> [destination <*dstIpv6Prefix*>] [flow <*ipv6Flow*>] } | { destination <*dstIpv6Prefix*> [flow <*ipv6Flow*>] } | { flow <*ipv6Flow*> }}] [l4-port {{ source <*l4SrcPort*> [destination <*l4DstPort*>] } | { destination <*l4DstPort*> }}] [tcp flags {ns | cwr | ece | urg | ack | psh | rst | syn | fin}] [dscp <*dscpVal*>] [cos <*cosVal*>] [tos <*tosVal*>] [ttl <*ttlVal*>] [l2-payload-head <*l2PayloadHeadVal*>] [vxlan vni <*vniBits*>]

access-list expression <*aclExpressionId*> vlan {{ outer {{ <*outerVlan*> [priority <*outerVlanPriority*>] [cfi <*outerVlanCfi*>] } | { priority <*outerVlanPriority*> [cfi <*outerVvlanCfi*>] } | { cfi <*outerVlanCfi*> }} [inner {{ <*innerVlan*> [priority <*innerVlanPriority*>] [cfi <*innerVlanCfi*>] } | { priority <*innerVlanPriority*> [cfi <*innerVlanCfi*>] } | { cfi <*innerVlanCfi*> }}] [format {untagged | tagged}] } | { inner {{ <innerVlan> [priority <*innerVlanPriority*>] [cfi <*innerVlanCfi*>] } | { priority <*innerVlanPriority*> [cfi <*innerVlanCfi*>] } | { cfi <*innerVlanCfi*> }} [format {untagged | tagged}] } | { format {untagged | tagged} }} [ethertype <*ethtype*>] [ip {{ source <*srcIp*> <*srcIpMask*> [destination <*dstIp*> <*dstIpMask*>] [protocol {<*protocolDecVal*> | {hopopt | icmp | igmp | ggp | ipv4 | st | tcp | cbt | egp | igp | bbn-rcc-mon | nvp-ii | pup | xnet | udp | dcn-meas | hmp | prm | rdp | irtp | iso-tp4 | netblt | mfe-nsp | merit-inp | dccp | 3pc | idpr | xtp | ddp | idpr-cmtp | tp++ | il | ipv6 | sdrp | ipv6-route | ipv6-frag | idrp | rsvp | gre | mhrp | esp | ah | i-nlsp | narp | tlsp | skip | ipv6-icmp | ipv6-nonxt | ipv6-opts | rvd | ippc | sat-mon | visa | ipcv | cpnx | cphb | wsn | pvp | br-sat-mon | vmtp | secure-vmtp | iptm | dgp | ospf | sprite-rpc | larp | mtp | ipip | micp | scc-sp | etherip | encap | ifmp | pim | aris | scps | ipcomp | snp | compaq-peer | vrrp | pgm | l2tp | ddx | iatp | stp | srp | smp | pipe | sctp | fc}}] [type {ipv4-any | ipv6-any | non-ip | {arp {request | reply}}}] [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { destination <*dstIp*> <*dstIpMask*> [protocol {<*protocolDecVal*> | {hopopt | icmp | igmp | ggp | ipv4 | st | tcp | cbt | egp | igp | bbn-rcc-mon | nvp-ii | pup | xnet | udp | dcn-meas | hmp | prm | rdp | irtp | iso-tp4 | netblt | mfe-nsp | merit-inp | dccp | 3pc | idpr | xtp | ddp | idpr-cmtp | tp++ | il | ipv6 | sdrp | ipv6-route | ipv6-frag | idrp | rsvp | gre | mhrp | esp | ah | i-nlsp | narp | tlsp | skip | ipv6-icmp | ipv6-nonxt | ipv6-opts | rvd | ippc | sat-mon | visa | ipcv | cpnx | cphb | wsn | pvp | br-sat-mon | vmtp | secure-vmtp | iptm | dgp | ospf | sprite-rpc | larp | mtp | ipip | micp | scc-sp | etherip | encap | ifmp | pim | aris | scps | ipcomp | snp | compaq-peer | vrrp | pgm | l2tp | ddx | iatp | stp | srp | smp | pipe | sctp | fc}}] [type {ipv4-any | ipv6-any | non-ip | {arp {request | reply}}}] [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { protocol {<*protocolDecVal*> | {hopopt | icmp | igmp | ggp | ipv4 | st | tcp | cbt | egp | igp | bbn-rcc-mon | nvp-ii | pup | xnet | udp | dcn-meas | hmp | prm | rdp | irtp | iso-tp4 | netblt | mfe-nsp | merit-inp | dccp | 3pc | idpr | xtp | ddp | idpr-cmtp | tp++ | il | ipv6 | sdrp | ipv6-route | ipv6-frag | idrp | rsvp | gre | mhrp | esp | ah | i-nlsp | narp | tlsp | skip | ipv6-icmp | ipv6-nonxt | ipv6-opts | rvd | ippc | sat-mon | visa | ipcv | cpnx | cphb | wsn | pvp | br-sat-mon | vmtp | secure-vmtp | iptm | dgp | ospf | sprite-rpc | larp | mtp | ipip | micp | scc-sp | etherip | encap | ifmp |

pim | aris | scps | ipcomp | snp | compaq-peer | vrrp | pgm | l2tp | ddx | iatp | stp | srp | smp | pipe | sctp | fc}} [type {ipv4-any | ipv6-any | non-ip | {arp {request | reply}}}] [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { type {ipv4-any | ipv6-any | non-ip | {arp {request | reply}}} [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { flags {df | mf} [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { fragment {no-frag | no-frag-or-head | head | sub | any} [header-size <*ipHeaderSize*>] } | { headerSize <*ipHeaderSize*> }}] [ipv6 {{ source <*srcIpv6Prefix*> [destination <*dstIpv6Prefix*>] [flow <*ipv6Flow*>] } | { destination <*dstIpv6Prefix*> [flow <*ipv6Flow*>] } | { flow <*ipv6Flow*> }}] [l4-port {{ source <*l4SrcPort*> [destination <*l4DstPort*>] } | { destination <*l4DstPort*> }}] [tcp flags {ns | cwr | ece | urg | ack | psh | rst | syn | fin}] [dscp <*DscpVal*>] [cos <*cosVal*>] [tos <*tosVal*>] [ttl <*ttlVal*>] [l2PayloadHead <*l2PayloadHeadVal*>] [vxlan vni <*vniBits*>]

access-list expression <*aclExpressionId*> ethertype <*ethtype*> [ip {{ source <*srcIp*> <*srcIpMask*> [destination <*dstIp*> <*dstIpMask*>] [protocol {<*protocolDecVal*> | {hopopt | icmp | igmp | ggp | ipv4 | st | tcp | cbt | egp | igp | bbn-rcc-mon | nvp-ii | pup | xnet | udp | dcn-meas | hmp | prm | rdp | irtp | iso-tp4 | netblt | mfe-nsp | merit-inp | dccp | 3pc | idpr | xtp | ddp | idpr-cmtp | tp++ | il | ipv6 | sdrp | ipv6-route | ipv6-frag | idrp | rsvp | gre | mhrp | esp | ah | i-nlsp | narp | tlsp | skip | ipv6-icmp | ipv6-nonxt | ipv6-opts | rvd | ippc | sat-mon | visa | ipcv | cpnx | cphb | wsn | pvp | br-sat-mon | vmtp | secure-vmtp | iptm | dgp | ospf | sprite-rpc | larp | mtp | ipip | micp | scc-sp | etherip | encap | ifmp | pim | aris | scps | ipcomp | snp | compaq-peer | vrrp | pgm | l2tp | ddx | iatp | stp | srp | smp | pipe | sctp | fc}}] [type {ipv4-any | ipv6-any | non-ip | {arp {request | reply}}}] [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { destination <*dstIp*> <*dstIpMask*> [protocol {<*protocolDecVal*> | {hopopt | icmp | igmp | ggp | ipv4 | st | tcp | cbt | egp | igp | bbn-rcc-mon | nvp-ii | pup | xnet | udp | dcn-meas | hmp | prm | rdp | irtp | iso-tp4 | netblt | mfe-nsp | merit-inp | dccp | 3pc | idpr | xtp | ddp | idpr-cmtp | tp++ | il | ipv6 | sdrp | ipv6-route | ipv6-frag | idrp | rsvp | gre | mhrp | esp | ah | i-nlsp | narp | tlsp | skip | ipv6-icmp | ipv6-nonxt | ipv6-opts | rvd | ippc | sat-mon | visa | ipcv | cpnx | cphb | wsn | pvp | br-sat-mon | vmtp | secure-vmtp | iptm | dgp | ospf | sprite-rpc | larp | mtp | ipip | micp | scc-sp | etherip | encap | ifmp | pim | aris | scps | ipcomp | snp | compaq-peer | vrrp | pgm | l2tp | ddx | iatp | stp | srp | smp | pipe | sctp | fc}}] [type {ipv4-any | ipv6-any | non-ip | {arp {request | reply}}}] [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { protocol {<protocolDecVal> | {hopopt | icmp | igmp | ggp | ipv4 | st | tcp | cbt | egp | igp | bbn-rcc-mon | nvp-ii | pup | xnet | udp | dcn-meas | hmp | prm | rdp | irtp | iso-tp4 | netblt | mfe-nsp | merit-inp | dccp | 3pc | idpr | xtp | ddp | idpr-cmtp | tp++ | il | ipv6 | sdrp | ipv6-route | ipv6-frag | idrp | rsvp | gre | mhrp | esp | ah | i-nlsp | narp | tlsp | skip | ipv6-icmp | ipv6-nonxt | ipv6-opts | rvd | ippc | sat-mon | visa | ipcv | cpnx | cphb | wsn | pvp | br-sat-mon | vmtp | secure-vmtp | iptm | dgp | ospf | sprite-rpc | larp | mtp | ipip | micp | scc-sp | etherip | encap | ifmp | pim | aris | scps | ipcomp | snp | compaq-peer | vrrp | pgm | l2tp | ddx | iatp | stp | srp | smp | pipe | sctp | fc}} [type {ipv4-any | ipv6-any | non-ip | {arp {request | reply}}}] [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { type {ipv4-any | ipv6-any | non-ip |

{arp {request | reply}}} [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { flags {df | mf} [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { fragment {no-frag | no-frag-or-head | head | sub | any} [header-size <*ipHeaderSize*>] } | { header-size <*ipHeaderSize*> }}] [ipv6 {{ source <*srcIpv6Prefix*> [destination <*dstIpv6Prefix*>] [flow <*ipv6Flow*>] } | { destination <*dstIpv6Prefix*> [flow <ipv6-flow>] } | { flow <*ipv6Flow*> }}] [l4-port {{ source <*l4SrcPort*> [destination <*l4DstPort*>] } | { destination <*l4DstPort*> }}] [tcp flags {ns | cwr | ece | urg | ack | psh | rst | syn | fin}] [dscp <*dscpVal*>] [cos <*cosVal*>] [tos <tosVal>] [ttl <*ttlVal*>] [l2-payload-head <*l2PayloadHeadVal*>] [vxlan vni <*vniBits*>]

access-list expression <*aclExpressionId*> ip {{ source <*srcIp*> <*srcIpMask*> [destination <*dstIp*> <*dstIpMask*>] [protocol {<*protocolDecVal*> | {hopopt | icmp | igmp | ggp | ipv4 | st | tcp | cbt | egp | igp | bbn-rcc-mon | nvp-ii | pup | xnet | udp | dcn-meas | hmp | prm | rdp | irtp | iso-tp4 | netblt | mfe-nsp | merit-inp | dccp | 3pc | idpr | xtp | ddp | idpr-cmtp | tp++ | il | ipv6 | sdrp | ipv6-route | ipv6-frag | idrp | rsvp | gre | mhrp | esp | ah | i-nlsp | narp | tlsp | skip | ipv6-icmp | ipv6-nonxt | ipv6-opts | rvd | ippc | sat-mon | visa | ipcv | cpnx | cphb | wsn | pvp | br-sat-mon | vmtp | secure-vmtp | iptm | dgp | ospf | sprite-rpc | larp | mtp | ipip | micp | scc-sp | etherip | encap | ifmp | pim | aris | scps | ipcomp | snp | compaq-peer | vrrp | pgm | l2tp | ddx | iatp | stp | srp | smp | pipe | sctp | fc}}] [type {ipv4-any | ipv6-any | non-ip | {arp {request | reply}}}] [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { destination <*dstIp*> <*dstIpMask*> [protocol {<*protocolDecVal*> | {hopopt | icmp | igmp | ggp | ipv4 | st | tcp | cbt | egp | igp | bbn-rcc-mon | nvp-ii | pup | xnet | udp | dcn-meas | hmp | prm | rdp | irtp | iso-tp4 | netblt | mfe-nsp | merit-inp | dccp | 3pc | idpr | xtp | ddp | idpr-cmtp | tp++ | il | ipv6 | sdrp | ipv6-route | ipv6-frag | idrp | rsvp | gre | mhrp | esp | ah | i-nlsp | narp | tlsp | skip | ipv6-icmp | ipv6-nonxt | ipv6-opts | rvd | ippc | sat-mon | visa | ipcv | cpnx | cphb | wsn | pvp | br-sat-mon | vmtp | secure-vmtp | iptm | dgp | ospf | sprite-rpc | larp | mtp | ipip | micp | scc-sp | etherip | encap | ifmp | pim | aris | scps | ipcomp | snp | compaq-peer | vrrp | pgm | l2tp | ddx | iatp | stp | srp | smp | pipe | sctp | fc}}] [type {ipv4-any | ipv6-any | non-ip | {arp {request | reply}}}] [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { protocol {<*protocolDecVal*> | {hopopt | icmp | igmp | ggp | ipv4 | st | tcp | cbt | egp | igp | bbn-rcc-mon | nvp-ii | pup | xnet | udp | dcn-meas | hmp | prm | rdp | irtp | iso-tp4 | netblt | mfe-nsp | merit-inp | dccp | 3pc | idpr | xtp | ddp | idpr-cmtp | tp++ | il | ipv6 | sdrp | ipv6-route | ipv6-frag | idrp | rsvp | gre | mhrp | esp | ah | i-nlsp | narp | tlsp | skip | ipv6-icmp | ipv6-nonxt | ipv6-opts | rvd | ippc | sat-mon | visa | ipcv | cpnx | cphb | wsn | pvp | br-sat-mon | vmtp | secure-vmtp | iptm | dgp | ospf | sprite-rpc | larp | mtp | ipip | micp | scc-sp | etherip | encap | ifmp | pim | aris | scps | ipcomp | snp | compaq-peer | vrrp | pgm | l2tp | ddx | iatp | stp | srp | smp | pipe | sctp | fc}} [type {ipv4-any | ipv6-any | non-ip | {arp {request | reply}}}] [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { type {ipv4-any | ipv6-any | non-ip | {arp {request | reply}}} [flags {df | mf}] [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { flags {df | mf} [fragment {no-frag | no-frag-or-head | head | sub | any}] [header-size <*ipHeaderSize*>] } | { fragment {no-frag | no-frag-or-head | head | sub | any} [header-size <*ipHeaderSize*>] } | {

header-size <*ipHeaderSize*> }} [ipv6 {{ source <*srcIpv6Prefix*> [destination <*dstIpv6Prefix*>] [flow <*ipv6Flow*>] } | { destination <*dstIpv6Prefix*> [flow <*ipv6Flow*>] } | { flow <*ipv6Flow*> }}] [l4-port {{ source <*l4SrcPort*> [destination <l4DstPort>] } | { destination <l4DstPort> }}] [tcp flags {ns | cwr | ece | urg | ack | psh | rst | syn | fin}] [dscp <*dscpVal*>] [cos <*cosVal*>] [tos <*tosVal*>] [ttl <*ttlVal*>] [l2-payload-head <*l2PayloadHeadVal*>] [vxlan vni <*vniBits*>]

access-list expression <*aclExpressionId*> ipv6 {{ source <*srcIpv6Prefix*> [destination <*dstIpv6Prefix*>] [flow <*ipv6Flow*>] } | { destination <*dstIpv6Prefix*> [flow <*ipv6Flow*>] } | { flow <*ipv6Flow*> }} [l4-port {{ source <*l4SrcPort*> [destination <l4DstPort>] } | { destination <*l4DstPort*> }}] [tcp flags {ns | cwr | ece | urg | ack | psh | rst | syn | fin}] [dscp <*dscpVal*>] [cos <*cosVal*>] [tos <*tosVal*>] [ttl <*ttlVal*>] [l2-payload-head <*l2PayloadHeadVal*>] [vxlan vni <*vniBits*>]

access-list expression <*aclExpressionId*> l4-port {{ source <*l4SrcPort*> [destination <*l4DstPort*>] } | { destination <*l4DstPort*> }} [tcp flags {ns | cwr | ece | urg | ack | psh | rst | syn | fin}] [dscp <*dscpVal*>] [cos <*cosVal*>] [tos <*tosVal*>] [ttl <*ttlVal*>] [l2-payload-head <*l2PayloadHeadVal*>] [vxlan vni <*vniBits*>]

access-list expression <*aclExpressionId*> tcp flags {ns | cwr | ece | urg | ack | psh | rst | syn | fin} [dscp <*dscpVal*>] [cos <*cosVal*>] [tos <*tosVal*>] [ttl <*ttlVal*>] [l2-payload-head <*l2PayloadHeadVal*>] [vxlan vni <*vniBits*>]

access-list expression <*aclExpressionId*> dscp <*dscpVal*> [cos <*cosVal*>] [tos <*tosVal*>] [ttl <*ttlVal*>] [l2PayloadHead <*l2PayloadHeadVal*>] [vxlan vni <*vniBits*>]

access-list expression <*aclExpressionId*> cos <*cosVal*> [tos <*tosVal*>] [ttl <*ttlVal*>] [l2-payload-head <*l2PayloadHeadVal*>] [vxlan vni <*vniBits*>]

access-list expression <*aclExpressionId*> tos <*tosVal*> [ttl <*ttlVal*>] [l2PayloadHead <*l2PayloadHeadVal*>] [vxlan vni <*vniBits*>]

access-list expression <*aclExpressionId*> ttl <*ttlVal*> [l2PayloadHead <*l2PayloadHeadVal*>] [vxlan vni <*vniBits*>]

access-list expression <*aclExpressionId*> l2-payload-head <*l2PayloadHeadVal*> [vxlan vni <*vniBits*>]

access-list expression <*aclExpressionId*> vxlan vni <*hex*>

no access-list expression <*expressionId*> [mac {{source [destination]} | destination}] [vlan {{ outer [{{ priority [cfi] } | { cfi }}] [inner [{{ priority [cfi] } | { cfi }}]] [format] } | { inner [{{ priority [cfi] } | { cfi }}] [format] } | { format }}] [ethertype] [ip {{ source [destination] [protocol] [type] [flags] [fragment] [header-size]

} | { destination [protocol] [type] [flags] [fragment] [header-size] } | { protocol [type] [flags] [fragment] [header-size] } | { type [flags] [fragment] [header-size] } | { flags [fragment] [header-size] } | { fragment [header-size] } | { header-size }}] [ipv6 {{ source [destination] [flow] } | { destination [flow] } | { flow }}] [l4-port {{ source [destination] } | { destination }}] [tcp flags] [dscp] [cos] [tos] [ttl] [l2-payload-head] [vxlan vni]

Command Modes Configuration Mode `(config)#`

Syntax Description

expression	Configure ACL expression entries.
aclExpressionId	access list number.
mac	Filter packets using MAC address.
srcMac	Specify source MAC address to be participated in filtering.
srcMacMask	Specify source MAC mask to be participated in filtering. If not specified 'FF:FF:FF:FF:FF:FF' to be used.
destination	Filter packets using destination MAC address.
dstMac	Destination MAC address to be participated in filtering.
dstMacMask	Destination MAC mask to be participated in filtering. If not specified 'FF:FF:FF:FF:FF:FF' to be used.
vlan	Filter packets using outer and inner VLAN ID, priority and CFI.
outer	Filter packets using outer VLAN ID priority and CFI.
outerVlan	Specify outer VLAN ID to be participated in filtering.
priority	Filter packets using outer VLAN priority.
outerVlanPriority	Specify outer VLAN priority to be participated in filtering.
cfi	Filter packets using outer VLAN CFI.
outerVlanCfi	Specify outer VLAN CFI to be participated in filtering.
inner	Filter packets using inner VLAN ID priority and CFI.
innerVlan	Specify inner VLAN ID to be participated in filtering.
innerVlanPriority	Specify inner VLAN priority to be participated in filtering.
cfi	Filter packets using inner VLAN CFI.
innerVlanCfi	Specify inner VLAN CFI to be participated in filtering.
format	Filter packets using VLAN format.
untagged	Set VLAN format to untagged.

tagged	Set VLAN format to tagged.
ethertype	Filter packets using ethertype.
ethtype	Specify ETHERTYPE to be participated in filtering.
ip	Filter packets using IPv4 options.
source	Filter packets using source IP address.
srcIp	Specify source IP address to be participated in filtering.
srcIpMask	Specify source IP mask to be participated in filtering.
destination	Filter packets using destination IP address.
dstIp	Specify destination IP address to be participated in filtering.
dstIpMask	Specify destination IP mask to be participated in filtering.
protocol	Filter packets using protocol encapsulated in IP packet.
protocolDecVal	Specify number of the protocol.
hopopt	IPv6 Hop-by-Hop Option.
icmp	Internet Control Message Protocol.
igmp	Internet Gateway Management Protocol.
ggp	Gateway to Gateway.
ipv4	IPv4 (encapsulation).
st	Internet Stream Protocol.
tcp	Transmission Control Protocol.
cbt	Core-based trees.
egp	Exterior Gateway Protocol.
igp	Interior Gateway Protocol.
bbn-rcc-mon	BBN RCC Monitoring.
nvp-ii	Network Voice Protocol.
pup	Xerox PUP.
xnet	Cross Net Debugger.
udp	User Datagram Protocol.
dcn-meas	DCN Measurement Subsystems.

hmp	Host Monitoring Protocol.
prm	Packet Radio Measurement.
rdp	Reliable Datagram Protocol.
irtp	Internet Reliable Transaction Protocol.
iso-tp4	ISO Transport Protocol Class 4.
netblt	Bulk Data Transfer Protocol.
mfe-nsp	MFE Network Services Protocol.
merit-inp	MERIT Internodal Protocol.
dccp	Datagram Congestion Control Protocol.
3pc	Third Party Connect Protocol.
idpr	Inter-Domain Policy Routing Protocol.
xtp	Xpress Transport Protocol.
ddp	Datagram Delivery Protocol.
idpr-cmtp	IDPR Control Message Transport Protocol.
tp++	TP++ Transport Protocol.
il	IL Transport Protocol.
ipv6	IPv4 to IPv6.
sdrp	Source Demand Routing Protocol.
ipv6-route	Routing Header for IPv6.
ipv6-frag	Fragment Header for IPv6.
idrp	Inter-Domain Routing Protocol.
rsvp	Resource Reservation Protocol.
gre	Generic Routing Encapsulation.
mhrp	Mobile Host Routing Protocol.
esp	Encapsulating Security Payload.
ah	Authentication Header.
i-nlsp	Integrated Net Layer Security Protocol.
narp	NBMA Address Resolution Protocol.

tlsp	Transport Layer Security Protocol (using Kryptonet key management).
skip	Simple Key-Management for Internet Protocol.
ipv6-icmp	ICMP for IPv6.
ipv6-nonxt	No Next Header for IPv6.
ipv6-opts	Destination Options for IPv6.
rvd	MIT Remote Virtual Disk Protocol.
ippc	Internet Pluribus Packet Core.
sat-mon	SATNET Monitoring.
visa	VISA Protocol.
ipcv	Internet Packet Core Utility.
cpnx	Computer Protocol Network Executive.
cphb	Computer Protocol Heart Beat.
wsn	Wang Span Network.
pvp	Packet Video Protocol.
br-sat-mon	Backroom SATNET Monitoring.
vmtp	Versatile Message Transaction Protocol.
secure-vmtp	Secure Versatile Message Transaction Protocol.
iptm	Internet Protocol Traffic Manager.
dgp	Dissimilar Gateway Protocol.
ospf	Open Shortest Path First.
sprite-rpc	Sprite RPC Protocol.
larp	Locus Address Resolution Protocol.
mtp	Multicast Transport Protocol.
ipip	IP-within-IP Encapsulation Protocol.
micp	Mobile Internetworking Control Protocol.
scc-sp	Semaphore Communications Sec. Pro.
etherip	Ethernet-within-IP Encapsulation.
encap	Encapsulation Header.

ifmp	Ipsilon Flow Management Protocol.
pim	Protocol Independent Multicast.
aris	IBM's ARIS (Aggregate Route IP Switching) Protocol.
scps	Space Communications Protocol Standards.
ipcomp	IP Payload Compression Protocol.
snp	Sitara Networks Protocol.
compaq-peer	Compaq Peer Protocol.
vrrp	Virtual Router Redundancy Protocol, Common Address Redundancy Protocol.
pgm	PGM Reliable Transport Protocol.
l2tp	Layer Two Tunneling Protocol Version 3.
ddx	D-II Data Exchange (DDX).
iatp	Interactive Agent Transfer Protocol.
stp	Schedule Transfer Protocol.
srp	SpectraLink Radio Protocol.
smp	Simple Message Protocol.
pipe	Private IP Encapsulation within IP.
sctp	Stream Control Transmission Protocol.
fc	Fibre Channel.
type	Filter packets using IP type.
ipv4-any	Set IP type to IPv4 any.
ipv6-any	Set IP type to IPv6 any.
non-ip	Set IP type to non IP.
arp	Specify ARP type.
request	Set IP type to ARP request.
reply	Set IP type to ARP reply.
flags	Specify IP flag(s).
df	Don't Fragment.
mf	More Fragments.

fragment	Filter packets using IP fragment.
no-frag	Filter packets that are marked as don't fragment.
no-frag-or-head	Filter packets that are marked as don't fragment or head fragment.
head	Filter packets that are marked as head fragment.
sub	Filter packets that are marked as sub fragment.
any	Filter packets any fragment.
header-size	Filter packets using packet header size.
ipHeaderSize	Specify packet header size to be participated in filtering.
egp	Exterior Gateway Protocol.
igp	Interior Gateway Protocol.
bbn-rcc-mon	BBN RCC Monitoring.
nvp-ii	Network Voice Protocol.
pup	Xerox PUP.
xnet	Cross Net Debugger.
udp	User Datagram Protocol.
dcn-meas	DCN Measurement Subsystems.
hmp	Host Monitoring Protocol.
prm	Packet Radio Measurement.
rdp	Reliable Datagram Protocol.
irtp	Internet Reliable Transaction Protocol.
iso-tp4	ISO Transport Protocol Class 4.
netblt	Bulk Data Transfer Protocol.
mfe-nsp	MFE Network Services Protocol.
merit-inp	MERIT Internodal Protocol.
dccp	Datagram Congestion Control Protocol.
3pc	Third Party Connect Protocol.
idpr	Inter-Domain Policy Routing Protocol.
xtp	Xpress Transport Protocol.

ddp	Datagram Delivery Protocol.
idpr-cmtp	IDPR Control Message Transport Protocol.
tp++	TP++ Transport Protocol.
il	IL Transport Protocol.
ipv6	IPv4 to IPv6.
sdrp	Source Demand Routing Protocol.
ipv6-route	Routing Header for IPv6.
ipv6-frag	Fragment Header for IPv6.
idrp	Inter-Domain Routing Protocol.
rsvp	Resource Reservation Protocol.
gre	Generic Routing Encapsulation.
mhrp	Mobile Host Routing Protocol.
esp	Encapsulating Security Payload.
ah	Authentication Header.
i-nlsp	Integrated Net Layer Security Protocol.
narp	NBMA Address Resolution Protocol.
tlsp	Transport Layer Security Protocol (using Kryptonet key management).
skip	Simple Key-Management for Internet Protocol.
ipv6-icmp	ICMP for IPv6.
ipv6-nonxt	No Next Header for IPv6.
ipv6-opts	Destination Options for IPv6.
rvd	MIT Remote Virtual Disk Protocol.
ippc	Internet Pluribus Packet Core.
sat-mon	SATNET Monitoring.
visa	VISA Protocol.
ipcv	Internet Packet Core Utility.
cpnx	Computer Protocol Network Executive.
cphb	Computer Protocol Heart Beat.

wsn	Wang Span Network.
pvp	Packet Video Protocol.
br-sat-mon	Backroom SATNET Monitoring.
vmtp	Versatile Message Transaction Protocol.
secure-vmtp	Secure Versatile Message Transaction Protocol.
iptm	Internet Protocol Traffic Manager.
dgp	Dissimilar Gateway Protocol.
ospf	Open Shortest Path First.
sprite-rpc	Sprite RPC Protocol.
larp	Locus Address Resolution Protocol.
mtp	Multicast Transport Protocol.
ipip	IP-within-IP Encapsulation Protocol.
micp	Mobile Internetworking Control Protocol.
scc-sp	Semaphore Communications Sec. Pro.
etherip	Ethernet-within-IP Encapsulation.
encap	Encapsulation Header.
ifmp	Ipsilon Flow Management Protocol.
pim	Protocol Independent Multicast.
aris	IBM's ARIS (Aggregate Route IP Switching) Protocol.
scps	Space Communications Protocol Standards.
ipcomp	IP Payload Compression Protocol.
snp	Sitara Networks Protocol.
compaq-peer	Compaq Peer Protocol.
vrrp	Virtual Router Redundancy Protocol, Common Address Redundancy Protocol.
pgm	PGM Reliable Transport Protocol.
l2tp	Layer Two Tunneling Protocol Version 3.
ddx	D-II Data Exchange (DDX).
iatp	Interactive Agent Transfer Protocol.

stp	Schedule Transfer Protocol.
srp	SpectraLink Radio Protocol.
smp	Simple Message Protocol.
pipe	Private IP Encapsulation within IP.
sctp	Stream Control Transmission Protocol.
fc	Fibre Channel.
type	Filter packets using IP type.
ipv4-any	Set IP type to IPv4 any.
ipv6-any	Set IP type to IPv6 any.
non-ip	Set IP type to non IP.
request	Set IP type to ARP request.
reply	Set IP type to ARP reply.
df	Don't Fragment.
mf	More Fragments.
fragment	Filter packets using IP fragment.
no-frag	Filter packets that are marked as don't fragment.
no-frag-or-head	Filter packets that are marked as don't fragment or head fragment.
head	Filter packets that are marked as head fragment.
sub	Filter packets that are marked as sub fragment.
any	Filter packets any fragment.
header-size	Filter packets using packet header size.
ipHeaderSize	Specify packet header size to be participated in filtering.
type	Filter packets using IP type.
srcIpv6Prefix	Specify IPv6 source address to be used for filtering.
dstIpv6Prefix	Specify IPv6 destination address to be used for filtering.
flow	Filter packets using IPv6 flow label.
ipv6Flow	Specify IPv6 flow label to be used for filtering.
l4SrcPort	Specify L4 source port to be used for filtering.

l4DstPort	Specify L4 destination port to be used for filtering.
ns	Filter packets using NS flag.
cwr	Filter packets using CWR flag.
ece	Filter packets using ECN-Echo flag.
urg	Filter packets using URG flag.
ack	Filter packets using ACK flag.
psh	Filter packets using PSH flag.
rst	Filter packets using RST flag.
syn	Filter packets using SYN flag.
fin	Filter packets using FIN flag.
dscp	Filter packets using DSCP value.
dscpVal	Specify DSCP value to be participated in filtering.
cos	Filter packets using CoS value.
cosVal	Specify CoS value to be participated in filtering.
tos	Filter packets using ToS value.
tosVal	Specify ToS value to be participated in filtering.
ttl	Filter packets using TTL value.
ttlVal	Specify TTL value to be participated in filtering.
l2-payload-head	Filter packets using firts 64 bits of L2 Payload Head.
l2PayloadHeadVal	Specify firts 64 bits of L2 Payload Head to be participated in filtering.
vxlan	Filters packets using VXLAN options.
vni	Filters packets by VXLAN network identifier.
vniBits	VXLAN network identifier.
hex	VXLAN network identifier.

Command Default

Examples

```
(config)#access-list expression 1 dscp 1 cos 1 tos 1 ttl 1
l2-payload-head 1
```

Revision 1.2

Related Commands

access-list icmp

Adds entries for an access list (ACL) to process ICMP (Internet Control Message Protocol) packets.

Command Syntax **access-list standard** <*accessListNumber*> **deny|permit icmp** <*source*> <*sourceMask*>**|any** <*destination*> <*destinationMask*>**|any [tos** <*tos*>**] [dscp** <*dscp*>**] [cos** <*cos*>**] [ttl** <*ttl*>**]**

Command Modes Configuration Mode `(config)#`

Syntax Description

standard	Configures standard access list entry.
accessListNumber	Access list number. Valid range for access list numbers is 1-16777216. .
permit	Permits access if conditions match.
deny	Denies access if conditions match.
icmp	Specifies the IP ICMP packets.
source	Source IP address from which the packet is being sent.
sourceMask	Mask bits to be applied to the source IP address.
any	Specifies any source IP address from which the packet is being sent.
destination	Destination IP address where the packet is being sent to.
destinationMask	Mask bits to be applied to the destination IP address.
any	Specifies any destination IP address where the packet is being sent to.
tos	Packets can be filtered by the service level type.
tos	Specifies a ToS value (0-15).
dscp	Packets can be filtered by the differentiated services codepoint value.
dscp	Specifies a DSCP value (0-63).
cos	Packets can be filtered by the CoS value.
cos	Specifies a CoS value (0-7).
ttl	Packets can be filtered by the time-to-live value.
ttl	Specifies a TTL value (0-255).

Command Default

Examples

```
(config)#access-list standard 102 deny icmp 1.1.1.1
255.255.255.0 2.2.2.2 255.255.255.1 tos 15 dscp 50 cos 3 ttl
100
(config)#access-list standard 103 permit icmp any any cos 6
```

Revision 1.2

Related Commands

```
show access-lists
show access-groups
```

access-list igmp

Adds entries for an access list (ACL) to process IGMP (Internet Group Management Protocol) packets.

Command Syntax **access-list standard <***accessListNumber***> deny|permit igmp <***source***> <***sourceMask***>|any <***destination***> <***destinationMask***>|any [tos <***tos***>] [dscp <***dscp***>] [cos <***cos***>] [ttl <***ttl***>]**

Command Modes Configuration Mode `(config)#`

Syntax Description

standard	Configures standard access list entry.
accessListNumber	Access list number. Valid range for access list numbers is 1-16777216. .
permit	Permits access if conditions match.
deny	Denies access if conditions match.
igmp	Specifies the IP IGMP packets.
source	Source IP address from which the packet is being sent.
sourceMask	Mask bits to be applied to the source IP address.
any	Specifies any source IP address from which the packet is being sent.
destination	Destination IP address where the packet is being sent to.
destinationMask	Mask bits to be applied to the destination IP address.
any	Specifies any destination IP address where the packet is being sent to.
tos	Packets can be filtered by the service level type.
tos	Specifies a ToS value (0-15).
dscp	Packets can be filtered by the differentiated services codepoint value.
dscp	Specifies a DSCP value (0-63).
cos	Packets can be filtered by the CoS value.
cos	Specifies a CoS value (0-7).
ttl	Packets can be filtered by the time-to-live value.
ttl	Specifies a TTL value (0-255).

Command Default

Examples

```
(config)#access-list standard 104 deny igmp 1.1.1.1
255.255.255.0 2.2.2.2 255.255.255.1 tos 15 dscp 50 cos 3 ttl
100
(config)#access-list standard 105 permit igmp any any ttl
100
```

Revision 1.2

Related Commands

`show access-lists`
`show access-groups`

access-list ip

Adds entries for an access list (ACL) to process IP (Internet Protocol) packets.

Command Syntax **access-list standard <*accessListNumber*> deny|permit ip <*source*> <*sourceMask*>|any <*destination*> <*destinationMask*>|any [tos <*tos*>] [dscp <*dscp*>] [cos <*cos*>] [ttl <*ttl*>]**

Command Modes Configuration Mode `(config)#`

Syntax Description

standard	Configures standard access list entry.
accessListNumber	Access list number. Valid range for access list numbers is 1-16777216. .
permit	Permits access if conditions match.
deny	Denies access if conditions match.
ip	Specifies the IP packets.
source	Source IP address from which the packet is being sent.
sourceMask	Mask bits to be applied to the source IP address.
any	Specifies any source IP address from which the packet is being sent.
destination	Destination IP address where the packet is being sent to.
destinationMask	Mask bits to be applied to the destination IP address.
any	Specifies any destination IP address where the packet is being sent to.
tos	Packets can be filtered by the service level type.
tos	Specifies a ToS value (0-15).
dscp	Packets can be filtered by the differentiated services codepoint value.
dscp	Specifies a DSCP value (0-63).
cos	Packets can be filtered by the CoS value.

cos	Specifies a CoS value (0-7).
ttl	Packets can be filtered by the time-to-live value.
ttl	Specifies a TTL value (0-255).

Command Default

Examples

```
(config)#access-list standard 106 deny ip 1.1.1.1
255.255.255.0 2.2.2.2 255.255.255.1 tos 10 dscp 40 cos 7 ttl
100
(config)#access-list standard 107 permit igmp any any cos 5
```

Revision 1.2

Related Commands

`show access-lists`
`show access-groups`

access-list mac

Adds entries for an access list (ACL) to process packets based on MAC addresses of target and sender host.

Command Syntax **access-list standard <***accessListNumber***> deny|permit mac any|<***senderMac***> <***senderMacMask***> any|<***targetMac***> <***targetMacMask***> [protocol <***ethertype***>] [vlan <***vlanId***>] [cos <***cos***>]**

Command Modes Configuration Mode `(config)#`

Syntax Description

standard	Configures standard access list entry.
accessListNumber	Access list number. Valid range for access list numbers is 1-16777216. .
permit	Permits access if conditions match.
deny	Denies access if conditions match.
mac	Specifies MAC address to match.
any	Specifies any sender MAC address.
senderMac	MAC address of the host sender.
senderMacMask	Mask of the host sender.
any	Specifies any target address.
targetMac	MAC address of the target host.
targetMacMask	Mask of the target host.
protocol	Specifies that packets can be filtered by the number of the protocol.
ethertype	Number of the protocol.

vlan	Specifies that packets can be filtered by the VLAN ID.
vlanId	VLAN ID (1-4094).
cos	Specifies that packets can be filtered by the CoS value.
cos	CoS value (0-7).

Command Default

Examples

```
(config)#access-list standard 500 deny mac f2:0d:db:d8:6c:4c
ff:ff:ff:ff:ff:ff any vlan 1
(config)#access-list standard 107 permit mac any any
protocol 0x8000
```

Revision 1.2

Related Commands

`show access-lists`
`show access-groups`

access-list policer

Configures ACL traffic policer.

Command Syntax **access-list policer <***policerId***> committed {{set {{dscp <***dscpVal***>} | {vlan {priority <***vlanPriority***>}}}} | drop | normal | trap-to-cpu} capacity <***capacityLimit***> rate <***rateLimit***> excess {{set {{dscp <***dscpVal***>} | {vlan {priority <***vlanPriority***>}}}} | drop | normal | trap-to-cpu} capacity <***capacityLimit***> rate <***rateLimit***>**

Command Modes Configuration Mode `(config)#`

Syntax Description

policer	Configures ACL traffic policer.
policerId	ACL traffic policer number. The range is 1-16777216.
committed	Configure commited capacity and rate limits.
set	Sets packet field.
dscp	Filters packets using DSCP value.
dscpVal	DSCP value. The range is 0-63.
vlan	Sets VLAN.
priority	Sets VLAN priority.
vlanPriority	VLAN priority to be set. The range is 0-7.
drop	Drops ACL traffic policer control packets.
normal	Redirects packet normally.

trap-to-cpu	Redirects packet to CPU.
capacity	Configures committed buffer capacity limit for storing queued packets.
capacityLimit	Committed buffer capacity limit number.
rate	Configures committed rate limit in kbps for traffic.
rateLimit	Committed rate limit value.
excess	Configures excess fields.
set	Sets packet field.
dscp	Filters packets using DSCP value.
dscpVal	DSCP value.
drop	Drops ACL traffic policer control packets.
normal	Redirects packet normally.
trap-to-cpu	Redirects packet to CPU.

Command Default

Examples

```
(config)#access-list policer 1 committed drop capacity 1
rate 1 excess drop capacity 1 rate 1
(config)#access-list policer 1 committed normal capacity 1
rate 1 excess normal capacity 1 rate 1
(config)#access-list policer 1 committed set dscp 1 capacity
1 rate 1 excess set dscp 1 capacity 1 rate 1
(config)#access-list policer 1 committed trap-to-cpu
capacity 1 rate 1 excess trap-to-cpu capacity 1 rate 1
```

Revision 1.2

Related Commands

`show access-lists`
`show access-groups`

access-list tcp

Adds entries for an access list (ACL) to process TCP (Transmission Control Protocol) packets.

Command Syntax **access-list standard <***accessListNumber***> deny|permit tcp <***source***> <***sourceMask***>|any [eq** <*sourcePort*>**] <***destination***> <***destinationMask***>|any [eq <***destinationPort***>] [tos <***tos***>] [dscp <***dscp***>] [cos <***cos***>] [ttl <***ttl***>]**

Command Modes Configuration Mode `(config)#`

Syntax Description

standard	Configures standard access list entry.

accessListNumber	Access list number. Valid range for access list numbers is 1-16777216. .
permit	Permits access if conditions match.
deny	Denies access if conditions match.
tcp	Specifies the TCP packets.
source	Source IP address from which the packet is being sent.
sourceMask	Mask bits to be applied to the source IP address.
any	Specifies any source IP address from which the packet is being sent.
eq	Specifies that only packets on a given port number should be matched.
sourcePort	Source TCP port number (0-65535).
destination	Destination IP address where the packet is being sent to.
destinationMask	Mask bits to be applied to the destination IP address.
any	Specifies any destination IP address where the packet is being sent to.
eq *destinationPort*	Destination TCP port number (0-65535).
tos	Packets can be filtered by the service level type.
tos	Specifies a ToS value (0-15).
dscp	Packets can be filtered by the differentiated services codepoint value.
dscp	Specifies a DSCP value (0-63).
cos	Packets can be filtered by the CoS value.
cos	Specifies a CoS value (0-7).
ttl	Packets can be filtered by the time-to-live value.
ttl	Specifies a TTL value (0-255).

Command Default

Examples

```
(config)#access-list standard 300 deny tcp any eq 100 any eq
300
(config)#access-list standard 110 permit tcp 1.1.1.1
255.255.255.0 any cos 6
```

Revision 1.2

Related Commands

`show access-lists`
`show access-groups`

access-list udp

Adds entries for an access list (ACL) to process UDP (User Datagram Protocol) packets.

Command Syntax

access-list standard <*accessListNumber*> deny|permit udp <*source*> <*sourceMask*>|any [eq <*sourcePort*>] <*destination*> <*destinationMask*>|any [eq <*destinationPort*>] [tos <*tos*>] [dscp <*dscp*>] [cos <*cos*>] [ttl <*ttl*>]

Command Modes

Configuration Mode	`(config)#`

Syntax Description

standard	Configures standard access list entry.
accessListNumber	Access list number. Valid range for access list numbers is 1-16777216. .
permit	Permits access if conditions match.
deny	Denies access if conditions match.
udp	Specifies the UDP packets.
source	Source IP address from which the packet is being sent.
sourceMask	Mask bits to be applied to the source IP address.
any	Specifies any source IP address from which the packet is being sent.
eq	Specifies that only packets on a given port number should be matched.
sourcePort	Source TCP port number (0-65535).
destination	Destination IP address where the packet is being sent to.
destinationMask	Mask bits to be applied to the destination IP address.
any	Specifies any destination IP address where the packet is being sent to.
eq *destinationPort*	Destination TCP port number (0-65535).
tos	Packets can be filtered by the service level type.
tos	Specifies a ToS value (0-15).
dscp	Packets can be filtered by the differentiated services codepoint value.
dscp	Specifies a DSCP value (0-63).
cos	Packets can be filtered by the CoS value.
cos	Specifies a CoS value (0-7).
ttl	Packets can be filtered by the time-to-live value.
ttl	Specifies a TTL value (0-255).

Command Default

Examples

```
(config)#access-list standard 300 deny udp any eq 100 any eq
300
(config)#access-list standard 110 permit udp 1.1.1.1
255.255.255.0 any cos 6
```

Revision 1.2

Related Commands

`show access-lists`
`show access-groups`

auto-shutdown

Changes system shut-down configuration.

Command Syntax **[no] auto-shutdown enable | {threshold** *<temp>***}**

Command Modes Global Configuration Mode `(config)#`

Syntax Description

enable	Enables system auto-shutdown.
threshold	Sets auto-shutdown threshold temperature.
temp	Specifies temperature to threshold. The range is 0-126.

Examples

```
#configure
(config) #auto-shutdown enable
(config) # auto-shutdown threshold 100
```

Revision 1.0.1

Related Commands

errdisable

This command configures the ErrDisable options.

Command Syntax

[no] errdisable detect cause {all | {<*applicationName***> <***error***>}}**
[no] errdisable recovery {{cause {all | {<*applicationName***> <***error***>}}} | {interval <***interval***>}}**

Command Modes Global Configuration Mode `(config)#`

Syntax Description

detect	Configures state of ErrDisable detection cause.

cause	Enables ErrDisable detection globally.
recovery	Configures state of ErrDisable detection cause.
cause	Configures the application to bring the interface out of the error-disabled (err-disabled) state and retries coming up.
all	Enables a timer to recover from all causes.
applicationName	Application name to enable ErrDisable detection for.
error	Application specific port error.
interval	Sets port auto-recovery timeout.
interval	Port auto-recovery timeout.

Examples

```
#configure
(config)#no errdisable detect cause all
(config)#no errdisable detect cause L2StpControlApp
bpduGuard(config)#no errdisable recovery cause all
(config)#no errdisable recovery interval
(config)#errdisable recovery cause all
config)#errdisable recovery cause L2StpControlApp bpduGuard
(config)#errdisable recovery interval 30
```

Revision 1.2

Related Commands

fan

Changes system fan configuration.

Command Syntax **[no] fan {**<*id*> **{state enable | test}} | {mode manual | auto} | {speed** <*speed*>*}*

Command Modes

Global Mode	Configuration	`(config)#`

Syntax Description

id	Specifies fan unit to configure.
state	Sets fan state.
enable	Enables the fan.
test	Puts the fan into test mode.
mode	Sets fan mode.

	manual	Allows setting fan speed manually.
	auto	Fan speed will be changed with temperature automatically.
	speed<*speed*>}	Sets fan speed (in percentage).

Examples

```
#configure
(config) #fan 1 speed 75
(config) #fan 1 state enable
(config) #fan 1 mode auto
```

Revision 1.0.1

Related Commands

monitor environment

interface (modes)

Accesses one of three interface configuration modes; the port interface mode (config-if *interfaceName*), the VLAN configuration mode (if-vlan *vlanNumber*), or the port channel mode (config-if) from the global configuration (config) mode. To return to the global configuration mode, use the **exit** command. For a list of command modes, see Command Modes.

The **no** form of the command removes specified port channel or VLAN interface and all associated configurations.

Command Syntax **interface** <*interfaceName*> | **vlan** <*vlanNumber*> | **port-channel** <*portChannel*>

[no] interface vlan <*vlanNumber*>**|** **port-channel** <*portChannel*>

Command Modes Global Configuration Mode `(config)#`

Syntax Description		
	interfaceName	Port interface name. For example **xe1**.
	vlanNumber	VLAN number. The range is from 1 to 4094.
	portChannel	Port channel number. The range is 3800 to 4094.

Examples

```
#configure
(config) #interface xe1
(config-if xe1) #?
(config-if xe1) #exit
(config) #
(if-vlan 2) #?
(if-vlan 2) #exit
(config) #
(config) #interface port-channel 3800
(config-if) #?
(config-if) #exit
(config) #no interface port-channel 3800
```

Revision 1.2

Related Commands

show interface (User)
show interface (Privileged)
show port-channel (User)
show port-channel (Privileged)
show vlan (User)
show vlan (Privileged)
show running-config

interface port-channel range

Enters Ethernet channel range configuration mode.

Command Syntax **interface port-channel range <***portChannelRange***>**

Command Modes Global Mode Configuration `(config)#`

Syntax Description *portChannelRange* Port channel range to configure.

Examples

```
#configure
(config)#interface port-channel range 3800-3801
(config-if-range)#
```

Revision 1.1

Related Commands

show interface (User)
show interface (Privileged)

interface range

Configures interface range and enters interface range configuration mode. The interface range must be formed of interfaces of the same type, for example:

interface range xe1-xe48

In order to form interface range of interfaces of different types, the following syntax must be used:
interface range xe1-xe10,xce1-xce10

The following syntax is invalid and will raise an error:
interface range xe1-qe100.

Command Syntax **interface range <***interfaceRange***>**

Command Modes Global Mode Configuration `(config)#`

Syntax Description *interfaceRange* Interface range.

Examples

```
#configure
(config)#interface range xe1-xe2
(config-if-range)#
```

Revision	1.2
Related Commands	`show interface (User)` `show interface (Privileged)`

ip address (config)

Configures system IP address.

Command Syntax	**ip address** *<ipAddress> <ipMask>*		
Command Modes	Global Mode	Configuration	`#configure` `(config) #`
Syntax Description	*ipAddress*		IP address to set.
	ipMask		Network mask for the interface.
Command Default	*ipAddress*		10.1.1.1
	ipMask		255.255.255.0
Examples	`(config)#ip address 1.1.1.1 255.255.255.0` `(config)#ip address 2.2.2.2 255.255.255.0`		
Revision	1.0.1		
Related Commands	`show running-config` `show system`		

ip default-gateway (config)

Configures system default gateway IP address.

Command Syntax	**ip default-gateway** *<ipAddress>*		
Command Modes	Global Mode	Configuration	`#configure` `(config) #`
Syntax Description	*ipAddress*		System gateway IP address.
Command Default	N/A		
Examples	`(config)#ip default-gateway 10.1.1.1`		
Revision	1.0.1		
Delivery Package	Basic		

Related Commands

ip address (config)
show running-config
show system

ip igmp snooping

Configures Internet Group Management Protocol (IGMP) parameters. IGMP snooping listens to IGMP conversations to obtain and maintain a table of links in need of IP multicast streams.

Note: To enable IGMP at the port interface level, you must also enable IGMP globally. You can however, configure IGMP for the ports without enabling IGMP globally, see `ip igmp`.

Command Syntax

[no] ip igmp snooping [{query-interval <*interval*>} | {querier-robustness <*value*>} | {unknown-action {broadcast | drop}}]
[no] ip igmp snooping router-alert

Command Modes

Global Mode	Configuration	`(config)#`

Syntax Description

ip	Global IP configuration.
igmp	Global IGMP configuration.
snooping	Enables interface monitor globally.
query-interval	Configures query interval time for non IGMP v3 multicast routers.
interval	Query interval time to set.
querier-robustness	Configures querier robustness variable for non IGMP v3 multicast routers.
value	Querier robustness variable value to set.
unknown-action	Sets action for unknown IGMP control packets.
broadcast	Forwards unknown IGMP control packets.
drop	Drops unknown IGMP control packets.
router-alert	Enable the router alert IP option checking in the incoming packets.

Command Default

igmp snooping	Disabled

Examples

```
ip igmp snooping
(config)#ip igmp snooping query-interval 1
(config)#ip igmp snooping querier-robustness 1
(config)#ip igmp snooping unknown-action broadcast
(config)#ip igmp snooping unknown-action drop
(config)#ip igmp snooping router-alert
```

Revision 1.1

Related Commands

ip (if-vlan)
ip igmp
show running-config
show interface (User)

lacp enable

Globally enables the reception of LACP PDUs and the dynamic aggregation of ports based on received LACP PDUs for all port channels.
Disabling LACP globally does not enable LACP configuration at the port level.

Command Syntax **[no] lacp**

Command Modes Global Configuration Mode `(config)#`

Examples

```
#configure
(config)#lacp enable
(config)#no lacp
```

Revision 1.2

Related Commands

`lacp`
`lacp system-priority`

lacp system-priority

Determines which switch sets LACP link control port priorities.

Command Syntax **lacp system-priority** *<priority>*

Command Modes Global Configuration Mode `(config)#`

Syntax Description		
	priority	Port channel associated Bridge Priority. The value must be in increments of 4096. All other values are rejected. The range is 0 to 61,440 in steps of 4096.

Command Default None

Examples

```
#lacp system-priority 12288
```

Revision 1.0.1

Related Commands

`lacp`
`lacp enable`

lldp (config)

Configures the global Link Layer Discovery Protocol (LLDP).
To view the current configuration, use the **show lldp** commands.

Command Syntax

lldp credits <*credits*>| **holdtime** <*holdtime*>| **reinit** <*delay*> | **timer** <*interval*> | **fast-init**<*txCount*>|**fast-tx** <*interval*>

no lldp {**credits**| **holdtime | reinit |timer | fast-int | fast-tx}**

Command Modes

Global Configuration Mode `(config)#`

Syntax Description

credits	The maximum number of consecutive LDPDUs that can be transmitted at any time. The range is 1 to 10.
holdtime	The time-to-live (TTL) for LLDP frames originating from the LLDP agent. The range is 1 to 100 seconds.
delay	The delay from when the *admin-status* object of a particular port becomes *disabled* until reinitialization is attempted. The range is 1 to 10 seconds.
interval	The transmission interval for LLDP frames originating from the LLDP agent. The range is 1 to 3600 seconds.
fast-init *txCount*	Determines the number of LLDPDUs that are transmitted during a fast transmission period. The range is 1-8.
fast-tx *interval*	Defines the time interval in timer ticks between transmissions during fast transmission periods. The range is 1 o 3600.

Command Default

credits *credits*	
holdtime	4
reinit *delay*	2
timer *interval*	30

Examples

```
(config) #lldp reinit 1
(config) #lldp fast-tx 5
(config) #lldp fast-init 8
```

Revision

1.0.1

Related Commands

show lldp
lldp (config-if)

mac-address-table multicast (config)

Configures multicast MAC address table.

Command Syntax

mac-address-table static <*macAddress*> **vlan** <*vlanNumber*> **interface {**<*interfacName*>|**port-channel** <*portChannel*>}

no mac-address-table static <*macAddress*> **vlan <***vlanNumber*>

[no] mac-address-table multicast <*macAddress*> vlan <*vlanNumber*> interface {<*interfaceName*> | {port-channel <*portChannel*>}}

Command Modes Global Configuration Mode `(config)#`

Syntax Description

multicast	Removes entry from multicast MAC address table.
macAddress	MAC address of the port.
vlanNumber	VLAN associated with the port. The range is 1 to 4094.
interfacName	Interface name of the port. For example, **xe1**.
vlan	Adds vlan to multicast MAC address table
interface	Adds interface to multicast MAC address table
port-channel	Adds Ethernet channel to multicast MAC address table
portChannel	Ethernet channel number which is being added to multicast MAC address table.

Examples

```
(config)#mac-address-table multicast 01:5E:00:00:00:00 vlan
1 interface xe1
(config)#mac-address-table multicast 01:5E:00:00:00:00 vlan
1 interface port-channel 3800
(config)#no mac-address-table multicast 01:5E:00:00:00:00
vlan 1 interface xe1
(config)#no mac-address-table multicast 01:5E:00:00:00:00
vlan 1 interface port-channel 3800
```

Revision 1.2

Related Commands

`show mac-address-table (User)`
`show mac-address-table (Privileged)`

mac-address-table static (config)

Adds entries to the static MAC address table.
To view the table entry for a specific MAC address, use the **show mac-address-table** *macAddress* command.

Command Syntax **mac-address-table static** <*macAddress*> **vlan** <*vlanNumber*> **interface {**<*interfacName*>|**port-channel** <*portChannel*>}

no mac-address-table static <*macAddress*> **vlan <***vlanNumber*>

Command Modes Global Configuration Mode `(config)#`

Syntax Description

static	Configures static MAC address table.
macAddress	MAC address of the port.
vlanNumber	VLAN associated with the port. The range is 1 to 4094.

interfacName	Interface name of the port. For example, **xe1**.
vlan	Adds vlan to multicast MAC address table
interface	Adds interface to multicast MAC address table
port-channel	Adds Ethernet channel to multicast MAC address table
portChannel	Ethernet channel number which is being added to multicast MAC address table.

Examples

```
#show mac-address-table
#configure
(config)#mac-address-table static 00:00:67:00:00:01 vlan 1
interface xe1
(config)#mac-address-table static 00:00:67:00:00:01 vlan 1
interface port-channel 3800
(config)#no mac-address-table static 00:00:00:00:00:01 vlan
1
```

Revision

1.1

Related Commands

`show mac-address-table (User)`
`show mac-address-table (Privileged)`

mls qos

Configures the Multi Layer Switching (MLS) Quality of Service (QoS) map parameters for all Class of Services (CoSs). The configuration modes are IEEE 802.1p (dot1p) and Differentiated Services Code Point (DSCP). The IEEE 802.1p mode defines service quality at the MAC level whereas DSCP mode defines service quality at the packet level.

Command Syntax

mls qos map {**dot1p-cos** <*cos0Dot1p*> <*cos1Dot1p*> <*cos2Dot1p*> <*cos3Dot1p*> <*cos4Dot1p*> <*cos5Dot1p*> <*cos6Dot1p*> <*cos7Dot1p*> | **dscp-cos** <*cos0Dscp*> <*cos1Dscp*> <*cos2Dscp*> <*cos3Dscp*> <*cos4Dscp*> <*cos5Dscp*> <*cos6Dscp*> <*cos7Dscp*>}

[no] mls qos map dot1p-cos|dscp-cos

Command Modes

Global Configuration Mode	`(config)#`

Syntax Description

cos0Dot1p to *cos7Dot1p*	Defines the Class of Service (CoS) to 802.1p map. The range is 0 to 7.
cos0Dscp to *cos7Dscp*	Defines the Class of Service (CoS) to Differentiated Services Code Point (DSCP) map. The range is 0 to 63.

Command Default

The interface port and map lists are empty.
The default CoS to dot1p map is 0/0, 1/1, 2/2, 3/3, 4/4, 5/5, 6/6, 7/7.
The default CoS to DSCP map is 0/0, 1/8, 2/16, 3/24, 4/32, 5/40, 6/48, 7/56.

Examples

```
#show mls qos bandwidth
#show mls qos bandwidth interface xe1
#show mls qos map dot1p-cos
#show mls qos map dscp-cos
```

```
#show mls qos scheduling
#show mls qos scheduling interface xe1
#configure
(config) #mls qos map dot1p-cos 7 1 2 3 4 5 6 0
(config) #mls qos map dscp-cos 0 7 15 23 31 39 47 55
(config) #no mls qos map dot1p-cos
(config) #no mls qos map dscp-cos
```

Revision 1.0.1

Related Commands

`mls qos map cos-bandwidth`
`mls qos trust`
`show mls qos`
`show running-config`

monitor source

Adds the specified source interface or several source interfaces for monitoring.

Command Syntax **[no] monitor source interface {<*interfaceRange*> | port-channel<*portChannel*> destination interface <*interfaceName*> mode {rx | {{tx | both} [original]} | redirect**

Command Modes Global Configuration Mode `(config)#`

Syntax Description

source interface	Configures the source interface(s).
interfaceRange	Interface name or interface names list separated by dash or commas.
port-channel	Configures port channel(s) as source interface(s).
portChannel	Port channel number or list of numbers separated by dash or commas.
destination interface *interfaceName*	Name of the destination interface.
mode	Configures the traffic direction in which to duplicate packets.
both original	Duplicates ingress and egress packets. **original** – duplicates original frames.
redirect	Redirects ingress frames from mirrored-port and drop ingress frames on it.
rx	Duplicates ingress frames from mirrored-port.
tx original	Duplicates mirrored-port egress frames **original** – duplicates original frames.

Examples

```
(config)#monitor source interface xe1-xe2 destination interface
xe3 mode tx original
(config)#monitor source interface xe1-xe2 destination interface
xe3 mode both original
(config)#monitor source interface xe1-xe2 destination interface
xe3 mode redirect
(config)#monitor source interface xe1-xe2 destination interface
xe3 mode rx
(config)#no monitor source interface xe1-xe2 destination
```

```
interface xe3 mode tx original
(config)#no monitor source interface xe1-xe2 destination
interface xe3 mode both original
(config)#no monitor source interface xe1-xe2 destination
interface xe3 mode redirect
(config)#no monitor source interface xe1-xe2 destination
interface xe3 mode rx
(config)#monitor source interface port-channel 3800 destination
interface xe3 mode tx original
(config)#monitor source interface port-channel 3800 destination
interface xe3 mode both original
(config)#monitor source interface port-channel 3800 destination
interface xe3 mode rx
(config)#no monitor source interface port-channel 3800
destination interface xe3 mode tx original
(config)#no monitor source interface port-channel 3800
destination interface xe3 mode both original
(config)#no monitor source interface port-channel 3800
destination interface xe3 mode rx
```

Revision 1.2

Related Commands `show monitor`

no interface port-channel

Removes the specified port interface from the port channel.

Command Syntax **no interface port-channel** *<channelNumber>*

Command Modes

Global Mode	Configuration	(config)#

Syntax Description

channelNumber	Port channel interface number. The range is 3800 to 4094.

Examples

```
(config)#interface port-channel 3800
(config-if)#exit
(config)#no interface port-channel 3800
(config)#
```

Revision 1.0.1

Related Commands

`show port-channel (User)`
`show port-channel (Privileged)`
`interface (modes)`

ovs bridge

Adds an Open-vSwitch bridge. The **no** form of the command deletes the specified bridge from switch configuration.

Command syntax	**ovs bridge add <** *bridgeName***>** **no ovs bridge [controller <***bridgeName***> [<***controllerName***>]]**	
Command Modes	Global Configuration Mode	`(config)#`
Syntax Description	*bridgeName*	Bridge name starts with 'spp' following by bridge-id (e.g.'spp0').
	controllerName	OpenFlow controller end-point.
Command Default	This command has no default settings.	
Examples	`(config)#ovs bridge add spp0`	
Revision	1.2	
Related Commands	`show ovs`	

ovs bridge controller

Configures OpenFlow controller for the specified bridge.

Command Syntax	**ovs bridge controller <** *bridgeName***> <** *ovsController***>**	
Command Modes	Global Configuration Mode	`(config)#`
Syntax Description	*bridgeName*	Bridge name starts with 'spp' following by bridge-id (e.g.'spp0').
	ovsController	OpenFlow controller end-point.
Command Default	This command has no default settings.	
Examples	`(config)#ovs bridge controller spp0 CON1`	
Revision	1.0.1	
Related Commands	`show ovs`	

ovs flow

Adds flow to the specified OpenFlow bridge. The **no** form of this command is used to remove the OpenFlow rule from the bridge.

Command Syntax	**ovs flow <***bridgeName***> <***flowId***> <***tableId***> [<***priority***>]**	
Command Modes	Global Configuration Mode	`(config)#`
Syntax Description	*bridgeName*	Bridge name starts with 'spp' following by bridge-id (e.g.'spp0').
	flowId	Flow ID to specify.
	tableId	Flow table ID to specify.
	priority	Priority value to specify.
Command Default	*priority*	32768
Examples	`(config)#ovs flow spp0 1 0 1`	
Revision	1.2	
Related Commands	`show ovs`	

ovs resources rules-limit

Limits the number of OpenFlow forwarding rules.

Command Syntax	**ovs resources rules-limit <*limitNumber*>**		
Command Modes	Global Mode	Configuration	`(config)#`
Syntax Description	*limitNumber*	Open-vSwitch rules limit. The range is from 0 to 4096.	
Examples	`(config)#ovs resources rules-limit 1000`		
Revision	1.0.1		
Related Commands	`show ovs`		

port-channel

A port channel bundles up to thirty one (31) individual interfaces into a group to provide increased bandwidth and redundancy. Port channeling also load balances traffic across these physical interfaces. The port channel stays operational as long as at least one physical interface within the port channel is operational.

Note: One or several (up to 15) algorithms can be used for distribution of incoming and outgoing packets:

```
(config)#port-channel load-balance dscp
(config)#port-channel load-balance dst-ip
(config)#port-channel load-balance dst-mac
(config)#exit
#show port-channel

MAC Address ............................ 00:08:A2:08:F1:E3
Priority ............................... 32768
Collector Maximum Delay ................ 10
Port Channel Status .................... Enabled
Load-balance ........................... Enabled
Load-balance Mode ...................... Dscp,DstIp,DstMac
LACP Status ............................ Enabled
```

If the algorithms that have been used need to be changed, the no form of the command is to be executed previously:

```
(config)#no port-channel load-balance
(config)#exit
#show port-channel

MAC Address ............................ 00:08:A2:08:F1:E3
Priority ............................... 32768
Collector Maximum Delay ................ 10
Port Channel Status .................... Enabled
Load-balance ........................... Enabled
Load-balance Mode ...................... None
LACP Status ............................ Enabled
```

Now the necessary algorithms can be used:

```
(config) #port-channel load-balance ether-type
(config) #port-channel load-balance inner-vlan-id
(config) #port-channel load-balance inner-vlan-pri
(config) #exit
#show port-channel

MAC Address ............................ 00:08:A2:08:F1:E3
Priority ............................... 32768
Collector Maximum Delay ................ 10
Port Channel Status .................... Enabled
Load-balance ........................... Enabled
Load-balance Mode ...................... EtherType,InnerVlanId,InnerVlanPri
LACP Status ............................ Enabled
```

Command Syntax

port-channel load-balance dscp |dst-ip | dst-mac | ether-type | inner-vlan-id | inner-vlan-pri | ip-protocol | ip6-flow | l4-dst-port | l4-scr-port | outer-vlan-id | outer-vlan-pri | src-ip | src-mac

port-channel collector-max-delay <*maxDelay*>

no port-channel load-balance

Command Modes

Global Configuration Mode `(config)#`

Syntax Description

load-balance	Determines the distribution of incoming and outgoing packets amongst the interfaces of a port channel. The no form of this command clears current load balance configuration.
dscp	Load balancing by IP DSCP.
dst-ip	Load balancing by destination IP address.
dst-mac	Load balancing by destination MAC address.
ether-type	Load balancing by ethertype.
inner-vlan-id	Load balancing by inner VLAN ID.
inner-vlan-pri	Load balancing by inner VLAN priority.
ip-protocol	Load balancing by IP protocol.
ip6-flow	Load balancing by IPv6 traffic flow.
l4-dst-port	Load balancing by Layer 4 destination port.
l4-scr-port	Load balancing by Layer 4 source port.
outer-vlan-id	Load balancing by outer VLAN ID.
outer-vlan-pri	Load balancing by outer VLAN priority.

src-ip	Load balancing by source IP address.
src-mac	Load balancing by source MAC address.
collector-max-delay *maxDelay*	Specifies the delivery delay of a frame received from an Aggregator Parser to its MAC client in tens of microseconds. The range is 0 to 65,535.

Command Default

Examples

```
(config) #interface port-channel 3800
(config-if)#exit
(config) #port-channel collector-max-delay 1000
(config) #port-channel load-balance src-mac
```

Revision 1.0.1

Related Commands

show port-channel

power-supply

Configures system power supply.

Command Syntax **power-supply {**<*id*> **state enable}|{voltage vdd {**<*voltage*>|**fault-clear|{mode manual|auto}}**

Command Modes

Global Configuration Mode	#configure (config) #

Syntax Description

id	Power supply ID.
state enable	Enables power supply.
voltage	Sets power supply output voltage.
vdd	Sets output voltage on switch core voltage supply.
voltage	Voltage to be set (mV). The range is 800-1300.
fault-clear	Clears power supply faults.
mode	Sets power supply output voltage mode.
manual	Allows setting power supply output voltage manually.
auto	Sets power supply output voltage automatically.

Command Default TBD

Examples

```
#show running-config
#configure
(config) #power-supply voltage vdd 800
```

```
(congig) #power-supply 1 state enable
```

Revision 1.0.1

Related Commands

spanning-tree (config)

Defines the spanning tree configuration parameters for the platform. BDPUs are used to exchange information about bridge IDs and root path costs.

Note: Changing spanning-tree modes affects traffic as all spanning-tree instances are stopped and restarted.

Command Syntax

spanning-tree {**forward-time** <*forwardTime*> | **max-age<***maxAgeTime*>| **max-hops** <*maxHopCount*> | **mode** {**mstp** | **rstp** | **stp**} |**mst configuration** | **priority** <*priority*> | **transmit hold-count**<*holdCount*>}
spanning-tree force-version {mstp|rstp|stp}
[no] spanning tree portfast bpduguard
[no] spanning-tree max-age
[no] spanning-tree forward-time
[no] spanning-tree max-hops
[no] spanning-tree priority
[no] spanning-tree transmit hold-count

Command Modes

Global Configuration Mode	`#configure` `(config) #`

Syntax Description

force-version	Sets the spanning-tree compatibility mode. This command forces the switch to emulate behaviour of earlier versions of spanning tree protocol, or return to MSTP behavior. The command is useful in test or debug applications, and removes the need to reconfigure the switch for temporary changes in spanning-tree operation.
mstp	The switch applies 802.1s operation on all ports except those ports where it detects a system using 802.1d Spanning Tree.
rstp	The switch applies 802.1w operation on all ports except those ports where it detects a system using 802.1d Spanning Tree.
stp	The switch applies 802.1d STP operation on all ports.
forward-time	Configures bridge forward delay time. The **no** form of the command configures bridge forward delay time to default value.
forwardTime	Interval spent listening for new information and learning new source addresses from received frames. The range is 4 to 30 seconds.
max-age	Configures STP bridge maximum age time. The **no** form of the command configures STP bridge maximum age time to default value.
maxAgeTime	Sets the interval between messages that the spanning tree receives from the root switch. The range is 6 to 40 seconds. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology.
max-hops	Configures STP maximum hops. The **no** form of the command configures STP maximum hops to default value.
maxHopCount	The maximum hop count before the BDPU is discarded. The range is 6 to 40.
mode	The spanning tree mode can be set to Multiple Spanning Tree (**mst**), Rapid Spanning Tree Protocol (**rstp**), or Spanning Tree Protocol (**stp**).
mstp	Sets spanning tree mode to MSTP.

rstp	Sets spanning tree mode to RSTP.
stp	Sets spanning tree mode to STP.
mst configuration	Enters the **mst** mode from the **configure** mode.
portfast	Configures STP PortFast BPDU Guard.
bpduguard	Configures PortFast BPDU Guard globally.
priority	Configures STP bridge Priority. The **no** form of the command configures STP bridge Priority to default value.
priority	Sets the STP bridge priority. The range is 0 to 61,440 in steps of 4,096.
transmit	Configures transmit BPDUs.
hold-count	Configures number of BPDUs sent every second. The **no** form of the command configures BPDUs sent every second to default value.
holdCount	Number of BPDUs sent every second.

Command Default

forwardTime	15 seconds
maxAgeTime	20 seconds
maxHopCount	20
mode	**RSTP**
priority	None
holdCount	6

Examples

```
(config)#no spanning-tree
(config)#spanning-tree priority 12288
(config)#spanning-tree forward-time 18
(config)#spanning-tree max-age 30
(config)#spanning-tree max-hops 10
(config)#spanning-tree transmit hold-count 10
(config)#spanning-tree mode stp
(config)#no spanning-tree max-age
(config)#no spanning-tree forward-time
(config)#no spanning-tree max-hops
(config)#no spanning-tree priority
(config)#no spanning-tree transmit hold-count
```

Revision 1.2

Related Commands

`show spanning-tree mst`
`spanning-tree (config-if)`
`spanning-tree mst configuration (mode)`

storm-control

Configures storm control options.

Command Syntax

storm-control {next-hop-miss | bpdu} level <*rateLimit*> <*bufferCapacityLimit*> **{ingress | egress }**

no storm-control {next-hop-miss | bpdu} [level {rate|capacity}] {ingress | egress }

Command Modes

Global Configuration Mode	`#configure` `(config) #`

Syntax Description

next-hop-miss	Configures next hop miss for storm control.
bpdu	Applies storm control to Bridge Protocol Data Units (BPDUs).
rateLimit	Rate limit in Kbps for traffic. The range is 1-40,000,000.
bufferCapacityLimit	Buffer capacity limit for storing queued packets. The range is 64 -1,000,000.
level	Sets storm suppression level on this interface.
ingress	Applies storm control to incoming traffic.
egress	Applies storm control to outgoing traffic.
capacity	Sets unlimited capacity buffer for storing queued packets.
rate	Sets unlimited rate buffer for traffic.

Command Default

rateLimit

bufferCapacityLimit

Examples

```
#show running-config
#configure
(config) #storm-control next-hop-miss level 24 64 egress
(config) #storm-control next-hop-miss level 24 64 ingress
(config) #storm-control bpdu level 24 64 egress
(config) #storm-control bpdu level 24 64 ingress
(config) #no storm-control next-hop-miss level capacity
ingress
(config) #no storm-control next-hop-miss level capacity
egress
(config) #no storm-control bpdu level rate ingress
(config) #no storm-control bpdu level rate egress
```

Revision

1.1

Related Commands

`storm-control (config-if, interface)`
`storm-control (config-if, port-channel)`

switch

Configures the aging time, default VLAN, and MAC address for the platform.

Command Syntax	**switch** {**aging-time** <*agingTime*> | **default-vlan** <*vlanNumber*> | **mac-address** <*macAddress*>}	
Command Modes	Global Configuration Mode	`#configure` `(config) #`
Syntax Description	*agingTime*	Global layer 2 aging time. The range is 10 to 1,000,000.
	vlanNumber	VLAN number. The range is 1 to 4094.
	macAddress	The platform MAC address.
Command Default	*agingTime*	300
	vlanNumber	1
	macAddress	None

Examples

```
#show running-config
#configure
(config) #switch aging-time 400
(config) #switch default-vlan 2
(config) #switch mac-address 00:00:67:00:00:01
```

Revision 1.0.1

Related Commands

`show running-config`

ufd

Configures a particular UFD group.

Command Syntax	**[no] ufd <*groupId*> [{enable | {threshold <*thresholdNumber*>}}]**

Command Modes

Global Configuration Mode	`#configure` `(config) #`
groupId	Integer value that uniquely represents the group number.
enable	Enables a particular UFD group.
threshold	Sets up the group threshold.
thresholdNumber	Minimum number of uplink ports that should be active to hold the downlink group in UfdUp status.

Command Default By default, group is created in disabled state.

Examples

```
(config)#ufd 1 enable
(config)#ufd 1 threshold 1
(config)#no ufd 1 enable
```

Revision 1.2

Related Commands `show ufd`

ufd enable

Enables UFD feature. The **no** form of the command disables UFD feature.

Command Syntax	**[no] ufd enable**

Command Modes

Global Configuration Mode	`#configure` `(config) #`
enable	Enables/disables UFD feature.

Command Default This command has no default values.

Examples

```
(config)#ufd enable
(config)#no ufd enable
```

Revision 1.2

Related Commands `show ufd`

ufd recovery-delay

Configures time that is needed for bringing up ports.

Command Syntax	**[no] ufd recovery-delay <***seconds***>**	
Command Modes	Global Configuration Mode	`#configure` `(config) #`
	recovery-delay	Configures time that is needed for bringing up ports.
	seconds	Minimum time that is needed for bringing up ports in downlink group.
Command Default	10 seconds	

Examples

```
(config)#ufd recovery-delay 20
(config)#no ufd recovery-delay
```

Revision 1.2

Related Commands `show ufd`

vlan (mode)

Enters the vlan simple configuration mode (config-vlan) from the global configuration mode (config). This mode enables the renaming of VLANs.

Command Syntax	**vlan** <*vlanNumber*>	
Command Modes	Global Configuration Mode	`(config)#`
Syntax Description	*vlanNumber*	VLAN number. The range is 1 to 4094.

Examples

```
#show vlan
#configure
(config) #vlan 2
(config-vlan) #?
(config-vlan) #exit
#
```

Revision 1.0.1

Related Commands

`name (config-vlan)`
`show vlan (User)`
`show vlan (Privileged)`
`vlan-database (mode)`
`switchport (config-if interface)`
`exit`

vlan dot1q tag native

Modifies the behavior of a 802.1Q trunked native VLAN ID interface. The interface maintains the taggings for all packets that enter with a tag that matches the value of the native VLAN ID and drops all untagged traffic. The control traffic is still carried on the native VLAN.

The vlan dot1q tag native command changes the behavior of all native VLAN ID interfaces on all trunks on the device.

The **no** form of the command disables egress traffic tagging on native (default) VLAN.

Command Syntax	**vlan dot1q tag native** **no vlan dot1q tag native**	
Command Modes	Global Configuration Mode	`(config)#`
Syntax Description	**vlan**	Configures VLANs.
	dot1q	Configures 801.1q tunnel.
	tag	Tags tunnel egress traffic.
	native	Enables egress traffic tagging on native(default) VLAN.
Command Default	Disabled.	

Examples

```
#configure
```

```
(config) #vlan dot1q tag native
(config) #no vlan dot1q tag native
```

Revision 1.2

Related Commands

`show vlan (User)`
`show vlan (Privileged)`
`vlan-database (mode)`
`switchport (config-if interface)`

6.4 Port Interface Configuration Mode Commands

access-group (config-if interface)

Sets inbound and outbound traffic control for a port based on the specified access lists. The **no** form of the command removes the specified access list, in and out, from the access group.

Command Syntax

access-group <*accessListRuleId*> **[**<*actionId*> <*expressionId*>**] {in | out}**
no access-group <*accessListRuleId*>

Command Modes

Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName) #
```

Syntax Description

accessListNumber	Access list number. Valid range for access list numbers is 1-16777216.
actionId	Action ID to participate in access list.
expressionId	Epression ID to participate in access list.
in	Filter on inbound packets.
out	Filter on outbound packets.

Command Default

Examples

```
(config) #interface xe1
(config-if xe1) #access-group 1 1 1 in
(config-if xe1) #access-group 1 1 1 out
(config-if xe1) #access-group 1 in
(config-if xe1) #access-group 1 out
(config-if xe1) #no access-group 1
```

Revision

1.2

Related Commands

`access-group (config-if, port-channel)`
`show running-config`
`show access-lists`

channel-group

The group of channel-group commands allows configuring Etherchannel/port bundling. After port is assigned to channel-group, all configuration for this port is cleared, e.g.: it is removed from participation in any Vlans, and static MAC definitions are removed. LAG configuration is applied for participated port.

Command Syntax

channel-group <*channelGroup*> {**aggregation** {**individual** | **multiple**}| **mode {active|passive}| {lacp port-priority** <*portPriority*>**}| timeout {short|long}| key** <*key*>**| collecting| defaulting| distributing| expired| synchronization| partner key** <*partnerKey*>**| partner number** <*partnerNumber*>**| partner priority** <*partnerPriority*>**| partner system**

<*macAddress*>| partner system priority <*partnerSystemPriority*>

no channel-group <*channelGroup*> **lacp port-priority|collecting| defaulting |defaulting| distributing| expired| synchronization**

Command Modes	Interface Configuration Mode	`#configure`
		`(config) #interface interfaceName`
		`(config-if interfaceName) #`

Syntax Description	*channelGroup*	Channel group number. The range is 3800 to 4094.
	aggregation	Specifies the aggregation mode for a channel group.
	individual	Specifies that the port may not be in a port channel with any other ports.
	multiple	Specifies that the port may be in a port channel with other ports.
	mode	Configures a channel group and a mode for the group.
	active	Enables LACP (Link Aggregation Control Protocol) unconditionally. This port sends periodic LACP PDUs.
	passive	Enables LACP only if a LACP device is detected. This port does not send periodic LACP PDUs.
	lacp port-priority *portPriority*	Configures the LACP port priority. LACP uses the port priority with the port number to form the port identifier. The **no** form of the command resets the port-priority to the default value.
	timeout	Specifies the interval between the transmission of LACP PDUs.
	short	Specifies a short interval.
	long	Specifies a long interval.
	key *key*	Assigns an administrative key value to the local port. The administrative key defines the ability of a port to aggregate with other ports. The range is 0 to 65535.
	collecting	Specifies the local port as collecting incoming frames.
	defaulting	Specifies the local port as defaulting.
	distributing	Specifies the local port as distributing.
	expired	Specifies the local port as being in the expired state.
	synchronization	Synchronizes the configuration of the port with the port channel configuration.
	partner key *partnerKey*	Sets the default value for the partner's key as assigned by the administrator or the system policy. The key is used when the partner's information is unknown or expired. The range is 0 to 65535.
	partner number *partnerNumber*	Sets the default value for the partner's number as assigned by the administrator or the system policy. The number is used when the partner's information is unknown or expired. The range is 0 to 65,535.

	partner priority *partnerPriority*	Sets the default value for the port priority component of the partner's port identifier as assigned by an administrator or the system policy. The priority is used when the partner's information is unknown or expired.
	partner system *macAddress*	Sets the default value for the MAC address component of the system identifier of the partner as assigned by an administrator or the system policy. The MAC address is used when the partner's information is unknown or expired.
	partner system priority *partnerSystemPriority*	Sets the default value for the system priority component of the system identifier as assigned by an administrator or the system policy. The priority is used when the partner's information is unknown or expired. The range is 0-15.
Command Default	**mode**	No channel groups are assigned.

TBD

Examples

```
(config) #interface xe1
(config-if xe1) #channel-group 3800 aggregation multiple
(config-if xe1) #channel-group 3800 collecting
(config-if xe1) #no channel-group 3800 collecting
(config-if xe1) #channel-group 3800 defaulting
(config-if xe1) #no channel-group 3800 defaulting
(config-if xe1) #channel-group 3800 distributing
(config-if xe1) #no channel-group 3800 distributing
(config-if xe1) #channel-group 3800 expired
(config-if xe1) #no channel-group 3800 expired
(config-if xe1) #channel-group 3800 key 65535
(config-if xe1) #channel-group lacp port-priority 65535
(config-if xe1) #channel-group 3800 mode active
(config-if xe1) #channel-group 3800 partner key 2
(config-if xe1) #channel-group 3800 partner number 4
(config-if xe1) #channel-group 3800 partner priority 300
 (config-if xe1) #channel-group 3800 partner system
00:00:0d:76:00:01
(config-if xe1) #channel-group 3800 partner system priority
4096
(config-if xe1) #channel-group 3800 synchronization
(config-if xe1) #no channel-group 3800 synchronization
(config-if xe1) # channel-group 3800 timeout short
```

Revision 1.2

Related Commands `show channel-group`

cut-through

The cut-through interface option allows packets to be transmitted on a port before the entire packet is received. This reduces the time a packet spends in the switch but increases the probability of transmit errors.

Command Syntax [**no**] **cut-through**

Command Modes

Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName)#
```

Command Default

Enabled.

Examples

```
#show interface xe1
#show interface
#configure
(config) interface xe1
(config-if xe1) #cut-through
(config-if xe1) #no cut-through
```

Revision

1.0.1

Related Commands

`show interface (User)`
`show interface (Privileged)`
`show statistics`

dcb

Data center bridging (DCB) is a port-level feature that provides enhancements to existing 802.1 bridge specifications to satisfy the requirements of protocols and applications in the data center. The DCB protocol enables 802.1 bridges to be used for the deployment of a network where all applications can be run over a single physical infrastructure.

The Data Center Bridging discovery and capability eXchange protocol (DCBX) conveys capabilities and configuration between neighbors to ensure consistent configuration across the network. DCBX leverages functionality provided by the Link Layer Discovery Protocol (LLDP) to exchange parameters between two link peers, using Type-Length-Values (TLVs).

DCB enhancements includes the following features:

- Congestion Notification (CN) provides end to end congestion management for protocols that do not have congestion control mechanisms built-in.
- Priority-based Flow Control (PFC) provides a link level flow control mechanism that can be controlled independently for each priority.
- Enhanced Transmission Selection (ETS) provides a common management framework for the assignment of bandwidth to traffic classes.
- Application Priority (APP) provides peer bridges to configure consistent mapping of Ethernet protocols to 802.1Q priorities.

The available DCBX protocol versions are as follows:

- DCBX Base Protocol v1.01 is the base DCBX protocol version.
- DCBX IEEE 802.1Qaz is the IEEE DCBX protocol version.

Note: The two DCBX versions are not compatible, thus both network elements must run the same version of DCBX.

Command Syntax

[no] dcb admin enable
[no] dcb app {willing | add {{ethertype <*protocol***>} | {tcp | udp | tcp-udp} <***protocol***>} <***priority***>}**
dcb cn {**cnpv-ready** | **cnpv-supported**} <*cnvpListNumber*>
dcb ets {**cbs** | **max-tcs** <*trafficClassNumber*>| **willing**}
[**no**] **dcb ets** {**cbs** | **willing**}
dcb ets-conf {**algorithm** <*algorithmListNumber*> | **bandwidth** <*bandwidthListNumber*>| **pri-assignment** <*trafficClassNumber*>}
dcb ets-reco {**algorithm** <*algorithmListNumber*> | **bandwidth** <*bandwidthListNumber*>| **pri-assignment** <*trafficClassNumber*>}
[**no**] **dcb pfc** {**mbc** | **priority** <*priorityListNumbers*>| **willing**}

[**no**] **dcb tx** {**all** | **app** | **cn** | **ets-conf** | **ets-reco** | **pfc**}

Command Modes	Interface Configuration Mode	`#configure`
		`(config) #interface` *`interfaceName`*
		`(config-if` *`interfaceName`*`) #`

Syntax Description	**admin**	Controls the administrative state of the port.
	app add	Adds an application priority mapping entry.
	protocolIndicator	Protocol indicator of the type indicated by the selector. The range is 1536 to 65,535.
	priorityCodePoint	Priority code point that should be used in frames transporting the protocol.
	ethertype, not-tcp-udp, tcp, tcp-udp, udp	Sets the selector type.
	algorithm *algorithmListNumber*	Configures the ETS algorithm. Enter eight values separated by commas. The range is 0 to 255.
	bandwidth *bandwidthListNumber*	Configures the ETS bandwidth. Bandwidth list values are separated by commas. The total of all eight octets must be equal to 100.
	cbs	Specifies if the Credit-Based Shaper Traffic Selection Algorithm is supported on the local system. Enter eight values. Each value can be 0 or 1. The values are separated by commas.
	cnpv-ready *cnvpListNumber*	Configures the Congestion Notification Priority Value *ready list* of congestion notifications. Enter eight values. Each value can be 0 or 1. The values are separated by commas.
	cnpv-supported *cnvpListNumber*	Configures the Congestion Notification Priority Value *supported list* for congestion notifications.
	max-tcs *trafficClassNumber*	Specifies the maximum number of traffic classes on the local device that may simultaneously have PFC enabled.
	mbc	Enables the local system to bypass MACsec (IEEE MAC Security standard) processing when MACsec is disabled.
	pri-assignment *trafficClassNumber*	Specifies the priority assignment list for ETS. A list of traffic classes to which the priority is assigned. A value of 15 indicates that the priority is not assigned to any traffic class. Enter eight values separated by commas. The range is 0 to 15.
	priority *priorityListNumbers*	Configures the PFC priority list which indicates the traffic classes on the local device when PFC is enabled. Enter eight values. Each value can be 0 (disabled) or 1 (enabled). The values are separated by commas.
	willing	This attribute indicates that the local system is willing to receive configuration information recommended by a remote system.
	tx	Enables the sending of PFC information in TLV messages.
Command Default	**admin**	None
	cbs	None
	mbc	None
	willing	None

protocol-version	**auto**
tx	app enabled, cn enabled, ets-conf enabled, pfc enabled, and ets-reco disabled.
cnvpListNumber	None
algorithmListNumber	None
bandwidthListNumber	None
pfcCapabilityNumber	1
priorityListNumbers	0,0,0,0,0,0,0,0
priorityCodePoint	None
protocolIndicator	None
trafficClassNumber	0

Examples

```
#show dcb app
#show dcb cn
#show dcb dcbx
#show dcb ets-conf
#show dcb ets-reco
#show dcb pfc
#configure
(config) #interface xe1
(config-if xe1) #dcb admin enable
(config-if xe1) #dcb tx pfc
(config-if xe1) #dcb tx ets-conf
(config-if xe1) #dcb tx ets-reco
(config-if xe1) #dcb tx app
(config-if xe1) #dcb tx cn
(config-if xe1) #dcb tx all
(config-if xe1) #dcb pfc willing
(config-if xe1) #dcb pfc mbc
(config-if xe1) #dcb pfc priority 0,0,1,0,0,0,0,0
(config-if xe1) #dcb ets willing
(config-if xe1) #dcb ets cbs
(config-if xe1) #dcb ets max-tcs 4
(config-if xe1) #dcb ets-conf bandwidth 5,5,5,5,10,20,20,30
(config-if xe1) #dcb ets-conf algorithm 5,5,5,25,25,25,25,2
(config-if xe1) #dcb ets-conf pri-assigment 1,1,1,1,1,1,1,15
(config-if xe1) #dcb ets-reco bandwidth 5,5,5,5,10,20,20,30
(config-if xe1) #dcb ets-reco algorithm 5,5,5,25,25,25,25,2
(config-if xe1) #dcb ets-reco pri-assigment 1,1,1,1,1,1,1,15
(config-if xe1) #dcb app willing
(config-if xe1) #dcb app add ethertype 1536 1
(config-if xe1) #dcb app add tcp 1 1
(config-if xe1) #dcb app add udp 1 1
(config-if xe1) #dcb app add tcp-udp 1 1
(config-if xe1) #no dcb app willing
(config-if xe1) #no dcb app add tcp 1 1
(config-if xe1) #no dcb app add udp 1 1
(config-if xe1) #no dcb app add tcp-udp 1 1
(config-if xe1) #dcb cn cnpv-supported 1,1,1,1,1,1,1,1
```

```
(config-if xe1) #dcb cn cnpv-ready 1,1,1,1,1,1,1,1
(config-if xe1) #no dcb tx pfc
(config-if xe1) #no dcb tx ets-conf
(config-if xe1) #no dcb tx ets-reco
(config-if xe1) #no dcb tx app
(config-if xe1) #no dcb tx cn
(config-if xe1) #no dcb tx all
(config-if xe1) #no dcb pfc willing
(config-if xe1) #no dcb pfc mbc
(config-if xe1) #no dcb pfc priority
(config-if xe1) #no dcb ets willing
(config-if xe1) #no dcb ets cbs
```

Revision 1.2

Related Commands

`show dcb`
`show running-config`

encapsulation dot1q

Controls stack VLAN processing on incoming Ethernet packets.
Note: The command is valid only if the interface is in customer-stacked mode.

Command Syntax

[no] encapsulation dot1q <*vlanId*> [<*vlanPriority*>]

Command Modes

Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName) #
```

Syntax Description

vlanId	Service provider VLAN identifier. The range is 1 to 4094.
vlanPriority	Service provider VLAN priority. The range is 0 to 7.

Examples

```
#configure
(config)# interface xe1
(config-if xe1)#switchport dot1qtunnel customer-stacked tpid
customer
(config-if xe1)#encapsulation dot1q 1 1
(config-if xe1)#no encapsulation dotq 1 1
```

Revision 1.2

Related Commands

`show dot1q-tunnel`
`show dot1q-tunnel`

flowcontrol

Determines if the interface processes received pause frames or sends pause frames (IEEE 802.3x). To view the current setting for an interface, use **show interface** *interfaceName* and observe the **Pause** field or use the **show running-config** and observe the **flowcontrol** fields of the interfaces. Flow control is achieved by sending a pause frame with the pause period embedded in the frame. The receiving end stops sending traffic for the specified period.

Command Syntax **flowcontrol {send | receive} {on | off}**

Command Modes Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName) #
```

Syntax Description

receive	When set to **off**, disables the processing of the pause frames.
send	When set to **off**, disables the transmission of pause frames.

Command Default Both receive and send pauses are enabled.

Examples

```
#show running-config
#show interface xe1
#configure
(config) #interface xe1
(config-if xe1) #flowcontrol receive off
(config-if xe1) #flowcontrol send off
(config-if xe1) #flowcontrol receive on
(config-if xe1) #flowcontrol send on
```

Revision 1.2

Related Commands

`show running-config`
`show interface flowcontrol`

ip igmp snooping

Configures interface-related IGMP options. The **no** form of the command negates IGMP options on interface.

Command Syntax

ip igmp snooping [router-port | stats clear]
no ip igmp snooping [router-port]

Command Modes Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName) #
```

igmp	Configures interface-related IGMP options.
snooping	Enables IGMP monitor on interface.
router-port	Configures the interface to be treated as connecting to a network with an IGMP multicast router.
stats clear	Clears all IGMP snooping statistics on the interface.

Command Default

Examples

```
(config-if xe1)#ip igmp snooping
(config-if xe1)#ip igmp snooping router-port
```

```
(config-if xe1)#ip igmp snooping stats clear
(config-if xe1)#no ip igmp snooping
(config-if xe1)#no ip igmp snooping router-port
```

Revision 1.0.1

Related Commands

`show ip imgp snooping`

lldp (config-if)

Configures the port interface Link Layer Discovery Protocol (LLDP).

Command Syntax

[no] lldp management-address {all802 | ipv4 | ipv6 } <*line*> {if-index | system-port-number | unknown} <*integer*> <*line*>

[no] lldp receive

[no] lldp tlv-select {management-address | port-description | system-capabilities | system-description | system-name}

[no] lldp transmit

Command Modes

Interface Configuration Mode	`#configure`
	`(config) #interface` *`interfaceName`*
	`(config-if xe1) #`

Syntax Description

management-address	Adds LLDP local management address on port.
all802	Address identifier type includes all 802 media plus Ethernet 'canonical format'.
ipv4	Address identifier type is IP Version 4.
ipv6	Address identifier type is IP Version 6.
line	Specify the string value used to identify the management address component associated with the local system.
if-index	Represents interface identifier based on the ifIndex MIB object.
system-port-number	Represents interface identifier based on the system port numbering convention.
unknown	Represents the case where the interface is not known.
integer	Integer value used to identify the interface number regarding the management address component associated with the local system.
line	The OID value used to identify the type of hardware component or protocol entity associated with the management address advertised by the local system agent.
receive	Enables the port to receive LLDP PDU’s.
tlv-select	Specifies the type length value (TLV)
management-address	Enables transmitting of the management address TLV messages.

port-description	Enables transmitting of the port description TLV messages.
system-capabilities	Enable transmitting of the system capabilities TLV messages.
system-description	Enable transmitting of the system description TLV messages.
system-name	Enable transmitting of the system name TLV messages.
transmit	Enables the port to transmit LLDP PDU’s.

Command Default

portDescription
Empty
receive
Enabled
tlv-select
All TLVs are enabled.
transmit
Enabled

Examples

```
#show running-config
#configure
(config) #interface xe1
(config-if xe1) #lldp receive
(config-if xe1) #lldp transmit
(config-if xe1) #lldp tlv-select management-address
(config-if xe1) #lldp tlv-select port-description
(config-if xe1) #lldp tlv-select system-capabilities
(config-if xe1) #lldp tlv-select system-description
(config-if xe1) #lldp tlv-select system-name
(config-if xe1) #no lldp receive
(config-if xe1) #no lldp transmit
(config-if xe1) #no lldp tlv-select management-address
(config-if xe1) #no lldp tlv-select port-description
(config-if xe1) #no lldp tlv-select system-capabilities
(config-if xe1) #no lldp tlv-select system-description
(config-if xe1) #no lldp tlv-select system-name
(config-if xe28)#lldp management-address all802
11:22:33:44:44:00 system-port-number 2 ""
(config-if xe28)#no lldp management-address all802
11:22:33:44:44:00 system-port-number 2 ""
(config-if xe28)#lldp management-address ipv4 10.2.3.2 if-
index 2 3.256.374.1
(config-if xe28)#no lldp management-address ipv4 10.2.3.2
if-index 2 3.256.374.1
(config-if xe28)#lldp management-address ipv6
fe80::208:a2ff:fe08:f1e7 unknown 0 1.235.488.644
(config-if xe28)#no lldp management-address ipv6
fe80::208:a2ff:fe08:f1e7 unknown 0 1.235.488.644
```

Revision 1.2

Related Commands

`show running-config`
`show lldp`
`lldp (config)`

mac-address (config-if interface)

Sets the MAC address of the port interface.

Command Syntax

mac-address <*macAddress*>

Command Modes

Port Channel Interface Configuration Mode

```
#configure
(config) #interface port-channel
portChannel
(config-if) #
```

Syntax Description

macAddress	MAC address of the port interface.

Command Default

None

Examples

```
#show interface xe1
#configure
(config) #interface xe1
(config-if xe1) #mac-address 00:23:45:67:89:AB
(config-if xe1) #no mac-address
```

Revision

1.0.1

Related Commands

`mac-address (config-if, port-channel)`
`show port-channel (User)`
`show port-channel (Privileged)`

mac-address-table (config-if)

Configures MAC address table learning mode.

Command Syntax

[no] mac-address-table learning-mode none|hardware

Command Modes

Interface Configuration Mode

```
(config-if) #
```

Syntax Description

learning-mode	Sets MAC address table learning mode on interface.
none	DLFs are not learned, frames are flooded on VLAN.
hardware	DLFs are learned by hardware, frames are flooded on VLAN.

Command Default

None

Examples

```
(config-if xe1)#mac-address-table learning-mode none
(config-if xe1)#mac-address-table learning-mode hardware
```

Revision

1.2

Related Commands

`show mac-address-table (User)`
`show mac-address-table (Privileged)`

mls qos map cos-bandwidth

Configures the Multi Layer Switching (MLS) Quality of Service (QoS) bandwidth for each Class of Service (CoS). During periods of congestion, the CoSs are serviced according to their configured bandwidth percentages.

Command Syntax [**no**] **mls qos map** {**cos-bandwidth** *<cos0Bandwidth> <cos1Bandwidth> <cos2Bandwidth> <cos3Bandwidth> <cos4Bandwidth> <cos5Bandwidth> <cos6Bandwidth> <cos7Bandwidth>*}

Command Modes Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName) #
```

Syntax Description

cos0Bandwidth to *cos7Bandwidth*	A value of 0 ensures that all packets for the specified CoS are dropped. A value of 100 or -1 ensures that no bandwidth limitation is implemented for the specified CoS. Any intermediate value ensures that a minimum bandwidth is allocated to the specified CoS. The range is 0 to100% for each CoS.

Command Default The CoS bandwidths are set to -1 for all CoSs. No bandwidth limitation.

Examples

```
#show running-config
#configure
(config) #interface xe1
(config-if xe1) #mls qos map cos-bandwidth 10 20 30 40 50 60
70 8
(config-if xe1) #no mls qos map cos-bandwidth
```

Revision 1.0.1

Related Commands

`mls qos trust`
`mls qos map`
`show running-config`

mls qos trust

Sets the Multi Layer Switching (MLS) port trust mode to either the 802.1p map or the Differentiated Code Services Point (DSCP) map.

Command Syntax [**no**] **mls qos trust** {**dot1p** | **dscp**}

Command Modes Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName) #
```

Syntax Description

dot1p	Sets the port trust mode to the 802.1p map.

dscp	Sets the port trust mode to the DSCP map.

Command Default No trust mode is assigned to the ports.

Examples

```
#show mls qos interface
#show mls qos maps
#configure
(config) # interface xe1
(config-if xe1) #mls qos trust dot1p
(config-if xe1) #mls qos trust dscp
(config-if xe1) #no mls qos trust
```

Revision 1.0.1

Related Commands

`mls qos map`
`mls qos map cos-bandwidth`
`show mls qos`
`show running-config`

ovs port add

Assigns the existing OpenFlow bridge to the port. The **no** form of the command is used to undo the assignment of the specified bridge to the port.

Command Syntax **[no] ovs port add <*bridgeName*>**

Command Modes Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName) #
```

Syntax Description

bridgeName	Bridge name starts with 'spp' following by bridge-id (e.g.'spp0').

Examples

```
(config)#interface xe1
(config)#ovs bridge add spp2
(config)#interface xe1
(config-if xe1)#ovs port add spp2
(config-if xe1)#
```

Revision 1.0.1

Related Commands

priority-queue

Sets scheduling algorithm mnemonic to Strict priority queue.

Command Syntax **priority-queue**

Command Modes Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName)#
```

Command Default Disabled.

Examples

```
(config-if xe1)#priority-queue
```

Revision 1.0.1

Related Commands

shutdown (port)

Controls the operational state of the port.

Command Syntax **[no] shutdown**

Command Modes Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName)#
```

Command Default Operational (not shutdown)

Examples

```
#show interface xe1
#show interface
#configure
(config) #interface xe1
(config-if xe1) #shutdown
(config-if xe1) #no shutdown
```

Revision 1.0.1

Related Commands

`show interface (User)`
`shutdown (VLAN interface)`

spanning-tree (config-if interface)

Defines the spanning tree configuration parameters for a port. BDPUs are used to exchange information about bridge IDs and root path costs.

Command Syntax **spanning-tree** {**bpduguard enable | cost** <*costNumber*> | **edge-port auto** | **enable** | **mac** |**mcheck | point-to-point-mac** {**force** | **not-force** | **auto**} **| portfast | priority <***priorityNumber***> | rootguard**}
no spanning-tree {bpduguard enable | edge-port auto | enable | mac |mcheck | point-to-point-mac | portfast | rootguard}

Command Modes Port Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName) #
```

Syntax Description

bpduguard enable	Enables BPDU Guard on port.
cost *costNumber*	Spanning tree path cost. The range is 1 to 200,000,000. A lower path cost represents a higher

		transmission speed.
	edge-port	Enables edge-port operation on the port to transition directly to the forwarding state. Use the **auto** option to enable automatic discovery of the edge ports.
	enable	Enables the spanning tree protocol on the port interface.
	mac	Enables support of the Internal Sublayer Service by specific MAC procedures.
	mcheck	Enables the port to send Rapid Spanning Tree (RST) BPDUs.
	point-to-point-mac	Configures the type of device connected to the port. **force** indicates a point-to-point link to a device such as a switch, bridge, or end-node. **not-force** indicates a connection to a hub which is a shared LAN segment. **auto** causes the switch to set Force-False on the port if it is not running at full duplex.
	priority	Configures spanning tree port priority.
	priorityNumber	Spanning tree priority. The range is 0 to 15.
	portfast	Enables Port Fast on port.
	rootguard	Enables Root Guard on port.
Command Default	**spanning-tree**	Enabled
	costNumber	2000
	edge-port	None
	point-to-point-mac	**force**

Examples

```
#show running-config
#configure
(config) #interface xe1
 (config-if xe1) #no spanning-tree bpduguard enable
(config-if xe1) #no spanning-tree edge-port
(config-if xe1) #no spanning-tree edge-port auto
(config-if xe1) #no spanning-tree enable
(config-if xe1) #no spanning-tree mac
(config-if xe1) #no spanning-tree mcheck
(config-if xe1) #no spanning-tree point-to-point-mac
(config-if xe1) #no spanning-tree portfast
(config-if xe1) #no spanning-tree rootguard
(config-if xe1)#spanning-tree cost 1000
(config-if xe1)#spanning-tree edge-port auto
(config-if xe1)#spanning-tree mac (config-if xe1)#spanning-
tree mcheck
(config-if xe1)#spanning-tree point-to-point-mac not-force
(config-if xe1)#spanning-tree priority 1
(config-if xe1)#spanning-tree enable
(config-if xe1)#spanning-tree bpduguard enable
(config-if xe1)#spanning-tree portfast
```

Revision	1.2

Related Commands	`show spanning-tree mst`
	`show running-config`
	`spanning-tree (config)`
	`spanning-tree mst configuration (mode)`

spanning-tree mst (config-if interface)

Defines the Multiple Spanning Tree (MST) configuration parameters for a port. BDPUs are used to exchange information about bridge IDs and root path costs.

Command Syntax

spanning tree mst <*mstInstance***> { bpduguard enable | edge-port auto | enable | external cost <***costNumber***>| internal cost <***costNumber***>| mac | mcheck | point-to-point-mac {auto|force|not-force}| portfast | priority <***priorityNumber***>| restricted-role | restricted-tcn | rootguard}**

no spanning tree mst <*mstInstance***> { bpduguard enable | edge-port auto | enable | mac | mcheck | point-to-point-mac | portfast | restricted-role | restricted-tcn | rootguard}**

Command Modes

Port Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName) #
```

Syntax Description

mstInstance	MST instance number. The range is 0 to 4094.
mst	Configures MST on the port.
mstInstance	MST instance on the port.
bpduguard enable	Configures BPDU Guard on port.
edge-port auto	Enables edge-port operation on the port.
enable	Enables MST on the port.
external cost	Configures MST instance external port cost.
internal cost	Configures MST instance internal port cost.
costNumber	MST instance internal or external cost value.
mac	Enables MAC-enabled feature on the port.
mcheck	Forces the port to send MST BPDUs.
point-to-point-mac	Configures the type of device connected to the port. **force** indicates a point-to-point link to a device such as a switch, bridge, or end-node. **not-force** indicates a connection to a hub which is a shared LAN segment. **auto** causes the switch to set Force-False on the port if it is not running at full duplex.

	portfast	Enables Port Fast on port.
	priority	Configures MST instance port priority.
	priorityNumber	Spanning tree priority. The range is 0 to 15.
	restricted-role	Enables MSTP restricted role.
	restricted-tcn	Enables MSTP restricted TCN.
	rootguard	Enables Root Guard on port.
Command Default	**spanning-tree**	Enabled

Examples

```
Switch #vlan-database
Switch (vlan)#vlan 10
Switch (config)#spanning-tree mst configuration
Switch (config-mst)#instance 10 vlan 10
#show spanning-tree
#show spanning-tree mst
#show running-config
#configure
(config) #interface xe1
(config-if) #no spanning-tree mst 10 bpduguard enable
(config-if) #no spanning-tree mst 10 portfast
(config-if) #no spanning-tree mst 10 rootguard
(config-if) #no spanning-tree mst 10 edge-port auto
(config-if) #no spanning-tree mst 10 mac
(config-if) #no spanning-tree mst 10 mcheck
(config-if) #no spanning-tree mst 10 point-to-point-mac
(config-if) #no spanning-tree mst 10 restricted-role
(config-if) #no spanning-tree mst 10 restricted-tcn
(config-if) #no spanning-tree mst 10 enable (config-
if)#spanning-tree mst 10 external cost 1000
(config-if)#spanning-tree mst 10 edge-port auto
(config-if)#spanning-tree mst 10 mac
(config-if)#spanning-tree mst 10 mcheck
(config-if)#spanning-tree mst 10 point-to-point-mac
not-force
(config-if)#spanning-tree mst 10 priority 1
(config-if)#spanning-tree mst 10 restricted-role
(config-if)#spanning-tree mst 10 restricted-tcn
(config-if)#spanning-tree mst 10 enable
(config-if)#spanning-tree mst 10 bpduguard enable
(config-if)#spanning-tree mst 10 portfast
(config-if)#spanning-tree mst 10 rootguard
```

Revision 1.2

Related Commands

`show spanning-tree mst`
`show running-config`
`spanning-tree (config)`
`spanning-tree mst configuration (mode)`

speed (config-if interface)

Sets the speed of the port in megabits/s (Mbps). The **no** command sets the port speed to non-negotiable and to 0 Mbps.

Command Syntax

speed {<*speed*> | auto | nonegotiate}

no speed

Command Modes

Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName)#
```

Syntax Description

speed	Sets speed value. The **no** form of the command sets default value for the interface speed configuration.
speed	Port speed in Mbps. The options are 1000, 2500, 10000, 40000.
auto	Enables autonegotiation on the interface. This is the default setting.
nonegotiate	Disables the autonegotiation on the interface. To restore autonegotiation, set the autonegotiate on the interface to Enable.

Command Default

The default port speed for all ports is 10,000.

Examples

```
(config-if xe1)#speed 1000
(config-if xe1)#speed auto
(config-if xe1)#speed nonegotiate(config-if xe1)#no speed
```

Revision

1.2

Related Commands

`show interface`

storm-control (config-if interface)

Configures the storm control parameters for a port based on the traffic type. A traffic storm occurs when packets flood a LAN, creating excessive traffic and degrading network performance. The traffic storm control feature prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm.

To view the current configuration, use the **show storm-control** command.

Storm control is invoked for a port when any of the configured rate limits *or* any of the buffer limits is exceeded. For example, the default configuration operates as follows:

- Limit ingress BPDUs on all ports to 1 Mbps or to a 4,096-byte buffer capacity.
- Limit ingress L3 packets without a next-hop destination on all ports to 1 Mbps or to a 4096-byte buffer capacity.

Upon exceeding any of the configured rate or buffer limits for a port, the packets are discarded until all limits are no longer exceeded.

Command Syntax

storm-control {**bdpu** | **broadcast** | **multicast** | **unicast**} **level**} <*rateLimitNumber*> <*bufferLimitNumber*> {**ingress** | **egress**}

no storm-control {**bdpu** | **broadcast** | **multicast** |**unicast**} **[level {capacity|rate}] {ingress | egress}**

Command Modes

Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName) #
```

Syntax Description

bdpu	Applies storm control to Bridge Protocol Data Units (BPDUs).
broadcast	Applies storm control to broadcast forwarding packets.
multicast	Applies storm control to multicast packets.
unicast	Applies storm control to unicast forwarding packets.
ingress	Applies storm control to incoming traffic.
egress	Applies storm control to outgoing traffic.
rateLimitNumber	The rate limit in kilobits/second (kbits/s). The range is 1 to 40,000,000.
bufferLimitNumber	The buffer limit in bytes. The range is 64 – 1,000,000.
level	Sets storm suppression level on this interface.
capacity	Sets unlimited capacity buffer for storing queued packets.
rate	Sets unlimited rate buffer for traffic.

Command Default

Both receive and send pauses are enabled.

Examples

```
#show storm-control
#configure
(config) #interface xe1
(config-if xe1) #storm-control broadcast level 2000000 64
ingress
(config-if xe1) #storm-control broadcast level 2000000 64
egress
 (config-if xe1) #no storm-control unicast level capacity
egress
(config-if xe1) #no storm-control unicast level capacity
ingress
(config-if xe1) #no storm-control unicast level rate egress
(config-if xe1) #no storm-control unicast level rate
ingress(config-if xe1) #no storm-control unicast ingress
(config-if xe1) #no storm-control unicast egress
```

Revision

1.2

Related Commands

`show storm-control`
`show running-config`
`show statistics`
`storm-control (config-if interface)`

switchport (config-if interface)

Sets the switching mode parameters for a port. The switchport parameters relate to packet discard mode, 802.1q tunneling (QinQ), ingress filtering, port priority, and port VLANs.

802.1q tunneling allows service providers to use a single VLAN to support multiple customer VLANs while preserving customer VLAN identifiers and segregating customer VLAN traffic.

To view the current configuration of the discard mode, ingress filtering, port default VLAN, and port default priority for all ports, use the **show interface** command.

To view the 802.1q tunneling and port VLAN assignments, use the **show running-config** command.

Command Syntax

[no] switchport {**discard** {**all** | **tagged** |**untagged**} | **ingress-filtering** | **pvid** <*vlanNumber*>| **pvpt** <*portPriority*>| **vlan add** <*vlanNumbers*> **tagged** | **untagged }**

no switchport {**discard** | **dot1qtunnel** | **pvid** | **pvpt** | **vlan {add** <*vlanNumbers*>} | {**mapping** <*customerVlanNumber*> <*customerPortPriority*> <*providerVlanNumber*> <*providerPortPriority*> }

[no] switchport dot1qtunnel {provider-mapped | provider-stacked} [tpid {customer | service | qinq}]

[no] switchport dot1qtunnel {customer-mapped | customer-stacked} [tpid customer]

Command Modes

Interface Configuration Mode

```
#configure
(config) #interface interfaceName
(config-if interfaceName) #
```

Syntax Description

all	Discards all incoming packets for the port.
tagged	Discards all incoming VLAN-tagged packets for the port.
untagged	Discards all incoming untagged packets for the port.
customer-stacked	Configure interface as customer stacked tunnel.
customer-mapped	Configure interface as customer mapped tunnel.
provider-mapped	Configure interface as provider mapped tunnel.
provider-stacked	Configure interface as provider stacked tunnel.
tpid	Configures tag protocol indetifier.
customer	Marks frames with Customer VLAN Tag, TPID: 0x8100.
service	Marks frames with Service VLAN Tag or Backbone VLAN Tag, TPID: 0x88A8.
qinq	Marks frames with QinQ legacy Tag, TPID 0x9100.
ingress-filtering	When ingress filtering is disabled, the port accepts any VLAN-tagged frame. When ingress filtering is enabled, incoming frames tagged for VLANs which do not include the ingress port are discarded.
pvid *vlanNumber*	Specifies the default VLAN identifier for the port. The range is 1 to 4094.
pvpt *portPriority*	Specifies the default VLAN priority for the port. The range is 0 to 15.

	vlan add *vlanNumbers*	Assigns one or more VLANs to the port. The range is 1 to 4094. Use commas to separate individual values and use dashes to list a range of contiguous VLANs.
	tagged	Supports tagged frames on interface.
	untagged	Supports untagged frames on interface.
Command Default	**discard**	None all for all ports.
	dot1qtunnel	None for all ports.
	ingress-filtering	None for all ports.
	pvid	VLAN 1 untagged for all ports.
	pvpt	Priority 0 for all ports.

Examples

```
#show running-config
#configure
(config) #interface xe1
(config-if xe1) #switchport discard all
(config-if xe1) #switchport discard tagged
(config-if xe1) #switchport discard untagged
(config-if xe1) #no switchport discard
 (config-if xe1) #switchport dot1qtunnel provider-mapped
 (config-if xe1) #switchport dot1qtunnel provider-mapped
tpid customer
(config-if xe1) #switchport dot1qtunnel provider-mapped tpid
service
(config-if xe1) #switchport dot1qtunnel provider-mapped tpid
qinq
  (config-if xe1) #switchport dot1qtunnel provider-stacked
tpid customer
(config-if xe1) #switchport dot1qtunnel provider-stacked
tpid service
(config-if xe1) #switchport dot1qtunnel provider-stacked
tpid qinq
(config-if xe1) #switchport dot1qtunnel customer-mapped
(config-if xe1) #switchport dot1qtunnel customer-mapped tpid
customer
(config-if xe1) #switchport dot1qtunnel customer-stacked
tpid customer
(config-if xe1) #no switchport dot1qtunnel
(config-if xe1) #switchport ingress-filtering
(config-if xe1) #switchport vlan add 2,4,100-102 tagged
(config-if xe1) #switchport vlan add 2,4,100-102 untagged
(config-if xe1) #switchport pvid 2
(config-if xe1) #switchport pvpt 1
(config-if xe1) #no switchport discard
config-if xe1) #no switchport dot1qtunnel
(config-if xe1) #no switchport ingress-filtering
(config-if xe1) #no switchport pvid
(config-if xe1) #no switchport pvpt
(config-if xe1) #no switchport vlan add 5-7
(config-if xe1) #no switchport vlan mapping 1 1 1 1
```

```
Switch #vlan-database
Switch (vlan)#vlan 200-300
Switch (vlan)#exit
Switch (config)#interface xe7
Switch (config-if xe7)#switchport dot1qtunnel customer-
mapped
Switch (config-if xe7)#switchport vlan mapping 201 1 301 3
```

Revision 1.2

Related Commands

`show interface (User)`
`show interface (Privileged)`
`show running-config`
`switchport (config-if, port-channel)`

ufd group (config-if)

Adds an interface to UFd group.

Command Syntax **[no] ufd group <*groupId*> {ltm | ltd}**

Command Modes

Interface Configuration Mode	`#configure`
	`(config) #interface interfaceName`
	`(config-if interfaceName)#`

group	Adds an interface to UFD group.
groupId	Integer value that uniquely represents the group.
ltm	Adds link to monitor interface to the specific UFD group.
ltd	Adds link to disable interface to the specific UFD group.

Command Default

Examples

```
(config-if xe1)#ufd group 1 ltm
(config-if xe1)#ufd group 1 ltd
(config-if xe1)#no ufd group 1 ltm
(config-if xe1)#no ufd group 1 ltd
```

Revision 1.2

Related Commands `show ufd`

ufd group (config-if-range)

Adds an interface to UFd group.

Command Syntax **[no] ufd group <*groupId*> {ltm | ltd}**

Command Modes

Interface Configuration Mode	#configure (config) #interface range *interfaceRange* (config-if-range)#
group	Adds an interface to UFD group.
groupId	Integer value that uniquely represents the group.
ltm	Adds link to monitor interface to the specific UFD group.
ltd	Adds link to disable interface to the specific UFD group.

Command Default

Examples

```
(config-if-range)#ufd group 1 ltm
(config-if-range)#ufd group 1 ltd
(config-if-range)#no ufd group 1 ltm
(config-if-range)#no ufd group 1 ltd
```

Revision 1.2

Related Commands `show ufd`

wrr-queue

Sets the scheduling mode to Weighted Deficit Round Robin (WRR) for the hardware output queues. The command defines the queue priorities in a congestion environment for each Class of Service (CoS). The ratio of the weights between CoSs defies how the WRR scheduler dequeues packets from each queue. The higher the bandwidth, the higher the CoS priority.

Command Syntax [**no**] **wrr-queue bandwidth** <*cos0BandwidthRatio*> <*cos1BandwidthRatio*> <*cos2BandwidthRatio*> <*cos3BandwidthRatio*> <*cos4BandwidthRatio*> <*cos5BandwidthRatio*> <*cos6BandwidthRatio*> <*cos7BandwidthRatio*>

Command Modes

Interface Configuration Mode	#configure (config) #interface *interfaceName* (config-if *interfaceName)* #

Syntax Description

cosXBandwidth	The CoS ratio for each of the 8 CoSs (X= 0 to 7). The range is 0 to 255.

Command Default

wrr-queue bandwidth	Disabled. The default scheduling mode is **Strict**.

Examples

```
#show mls qos interface
#configure
(config) #interface xe1
(config-if xe1) #wrr-queue bandwidth 10 20 30 40 50 60 70 80
(config-if xe1) #no wrr-queue bandwidth
```

Revision 1.0.1

Related Commands

```
show mls qos
mls qos map cos-bandwidth
mls qos map
```

6.5 VLAN Interface Configuration Mode Commands

vlan

Enables the creation and deletion of VLANs.
To view the current VLANs, use the **show vlan** command.

Command Syntax	**vlan**<*vlanNumber*>	
Command Modes	VLAN Interface Configuration Mode	`#vlan-database` `(vlan) #`
Syntax Description	*vlanNumber*	VLAN to create or delete. The range is 1 to 4094.

Examples

```
#show vlan
#vlan-database
(vlan) #vlan 100
(vlan) #vlan 2
(vlan) #no vlan 100
```

Revision 1.0.1

Related Commands

`show vlan (User)`
`vlan-database (mode)`
`wrr-queue`
`interface (modes)`
`switchport (config-if interface)`

6.6 Port Channel Interface Configuration Mode Commands

access-group (config-if, port-channel)

Sets inbound and outbound traffic control for a port based on the specified access lists. The **no** form of the command removes the specified access list, in and out, from the access group.

Command Syntax

access-group <*accessListRuleIdr***> [<***actionId***> <***expressionId***>] {in | out}**
no access-group <*accessListRuleId***>**

Command Modes

Port-Channel Configuration Mode	`#config`
	`(config) #interface port-channel channelNumber`
	`(config-if) #`

Syntax Description

accessListNumber	Access list number.
actionId	Action ID to participate in access list.
expressionId	Epression ID to participate in access list.
in	Filter on inbound packets.
out	Filter on outbound packets.

Command Default

Examples

```
(config) #interface xe1
(config-if 3800) #access-group 1 1 1 in
(config-if 3800) #access-group 1 1 1 out
(config-if 3800) #access-group 1 in
(config-if 3800) #access-group 1 out
(config-if 3800) #no access-group 1
```

Revision 1.2

Related Commands

`access group (config-if interface)`
`show running-config`
`show access-lists`

cut through

Enables transmission of a frame before the frame has been completely received.

Command Syntax **[no] cut through**

Command Modes

Port-Channel Configuration Mode

```
#config
(config) #interface port-channel
channelNumber
(config-if) #
```

Examples

```
#configure
(config)#interface port-channel 3800
(config-if 3800)#cut-through
(config-if 3800)#no cut-through
```

Revision 1.1

Related Commands

encapsulation dot1q

Controls stack VLAN processing on incoming Ethernet packets.

Command Syntax

[no] encapsulation dot1q <*vlanId*> [<*vlanPriority*>]

Command Modes

Port Channel Interface Configuration Mode

```
#configure
(config) #interface port-channel
portChannel
(config-if) #
```

Syntax Description

vlanId	Service provider VLAN identifier. The range is 1 to 4094.
vlanPriority	Service provider VLAN priority. The range is 0 to 7.

Examples

```
#configure
(config)# interface port-channel 3800
(config-if 3800)# encapsulation dot1q 1 1
(config-if 3800)# no encapsulation dotq 1 1
```

Revision 1.0.1

Related Commands

`show dot1q-tunnel`
`show dot1q-tunnel encapsulation`

ip igmp

Enables or disables the Internet Group Management Protocol (IGMP) for the interface. IGMP snooping listens to IGMP conversations to obtain and maintain a table of links in need of IP multicast streams.

Note: To enable IGMP at the port channel interface level, you must also enable IGMP globally, see `ip igmp snooping`. You can however, configure IGMP for the port channels without enabling IGMP globally.

Command Syntax

ip igmp snooping [router-port | stats clear]
no ip igmp snooping router-port

Command Modes

Port Channel Interface Configuration Mode

```
#configure
(config) #interface port-channel
portChannel
(config-if) #
```

Command Default

Disabled.

Examples

```
#show port-channel interfaces local
#configure
(config) #interface port-channel 3800
(config-if 3800) #ip igmp snooping
(config-if 3800) #ip igmp snooping router-port
(config-if 3800) #ip igmp snooping stats clear
(config-if 3800) #no ip igmp snooping router-port
```

Revision

1.2

Related Commands

`show port-channel (User)`
`show port-channel (Privileged)`
`show ip igmp`

key

Specifies the administrative key value associated with the port channel.

Command Syntax

key <*channelKey*>

Command Modes

Port Channel Interface Configuration Mode

```
#configure
(config) #interface port-channel
portChannel
(config-if) #
```

Syntax Description

channelKey	Port channel key. The range is 0 to 65,535.

Command Default

channelKey	Equals to channel number. For example, for **lag3800 administrative** key is 3800.

Examples

```
#show port-channel interfaces local
#configure
(config) #interface port-channel 3800
(config-if 3800) #key 1000
```

Revision

1.0.1

Related Commands

`show port-channel (User)`
`show port-channel (Privileged)`

lacp

Enables and disables the port channel from processing Received LACP (Link Aggregation Control Protocol) PDUs.

Command Syntax [**no**] **lacp**

Command Modes Port Channel Interface Configuration Mode

```
#configure
(config) #interface port-channel
portChannel
(config-if) #
```

Command Default Disabled.

Examples

```
#show port-channel interfaces local
#configure
(config) #interface port-channel 3800
(config-if 3800) #lacp
(config-if 3800) #no lacp
```

Revision 1.0.1

Related Commands

`show port-channel (User)`
`show port-channel (Privileged)`

mac-address (config-if, port-channel)

Sets the MAC address of the port channel.

Command Syntax **mac-address** <*macAddress*>

Command Modes Port Channel Interface Configuration Mode

```
#configure
(config) #interface port-channel
portChannel
(config-if) #
```

Syntax Description *macAddress* MAC address of the port channel.

Command Default None

Examples

```
#show port-channel local interfaces
#configure
(config) #interface port-channel 3800
(config-if 3800) #mac-address 01:23:45:67:89:AB
(config-if 3800) #no mac-address
```

Revision 1.0.1

Related Commands

`mac-address (config-if interface)`
`show port-channel (User)`
`show port-channel (Privileged)`

mac-address-table learning-mode

Configures the MAC address table learning mode.

Command Syntax

mac-address-table learning mode none | hardware
[no] mac-address-table learning mode

Command Modes

Port Channel Interface Configuration Mode

```
#configure
(config) #interface port-channel
portChannel
(config-if) #
```

learning-mode	Sets MAC address table learning mode on interface.
none	DLFs are not learned, frames are flooded on VLAN.
hardware	DLFs are learned by hardware, frames are flooded on VLAN.

Examples

```
#configure
(config)#interface port-channel 3800
(config-if 3800)#mac-address-table learning-mode none
(config-if 3800)#mac-address-table learning-mode hardware
(config-if 3800)#no mac-address-table learning-mode
```

Revision 1.2

Related Commands

max-frame-size (config-if, port-channel)

Configures the maximum frame size, in bytes, that a port channel can transmit. Larger frames must be fragmented before transmission. The parameter is Maximum Frame Size.

Command Syntax

[**no**] **max-frame-size** <*maximumFrameSize*>

Command Modes

Port Channel Interface Configuration Mode

```
#configure
(config) #interface port-channel
portChannel
(config-if) #
```

Syntax Description	*maximumFrameSize*	Maximum frame size in bytes. The range is 64 to 15864.
Command Default	*maximumFrameSize*	1522

Examples

```
#show port-channel local interfaces
#configure
(config) #interface port-channel 3800
(config-if 3800) # max-frame-size 64
(config-if 3800) # max-frame-size 15864
(config-if 3800) #no max-frame-size
```

Revision 1.0.1

Related Commands `show port-channel (User)` `show port-channel (Privileged)`

name (config-if, port-channel)

Sets the LAG name.

Command Syntax **name** <*portChannelName*>

Command Modes Port Channel Interface Configuration Mode

```
#configure
(config) #interface port-channel portChannel
(config-if) #
```

Syntax Description	*portChannelName*	Any continuous string of characters that can be entered from the keyboard. Up to 32 characters. No spaces.
Command Default	*portChannelName*	**lag***channelNumber.* For example, **lag3800.**

Examples

```
#show port-channel local interfaces
#configure
(config) #interface port-channel 3800
(config-if 3800) #name MyPortChannel_3800
(config-if 3800) #no name
```

Revision 1.0.1

Related Commands

`show port-channel (User)`
`show port-channel (Privileged)`

spanning-tree (config-if, port-channel)

Defines the spanning tree configuration parameters for a port. BDPUs are used to exchange information about bridge IDs and root path costs.

Command Syntax

spanning-tree {**bpduguard enable | cost** <*costNumber*> | **edge-port** [**auto**] | **enable** | **mac** |**mcheck** | **point-to-point-mac** {**force** | **not-force** | **auto**} | **portfast** | **priority** <*priorityNumber*> | **rootguard**}

no spanning-tree {**bpduguard enable** | **edge-port** [**auto**] | **enable** | **mac** |**mcheck** | **point-to-point-mac** | **portfast** | **rootguard**}

Command Modes Port Channel Interface Configuration Mode

```
#configure
(config) #interface port-channel portChannel
(config-if) #
```

Syntax Description	**bpduguard enable**	Enables or disables BPDU Guard on port.
	cost *costNumber*	Spanning tree path cost. The range is 1 to 200,000,000. A lower path cost represents a higher transmission speed.
	edge-port	Enables edge-port operation on the port to transition directly to the forwarding state. Use the

		auto option to enable automatic discovery of the edge ports.
	enable	Enables the spanning tree protocol on the port interface.
	mac	Specifies the port as MAC enabled.
	mcheck	Enables the port to send Rapid Spanning Tree (RST) BPDUs.
	point-to-point-mac	Configures the type of device connected to the port. **force** indicates a point-to-point link to a device such as a switch, bridge, or end-node. **not-force** indicates a connection to a hub which is a shared LAN segment. **auto** causes the switch to set Force-False on the port if it is not running at full duplex.
	portfast	Enables or disables PortFast on port.
	priority	Configures the type of the device to which the port connects.
	priorityNumber	Spanning tree priority. The range is 0 to 15.
	rootguard	Enables or disables Root Guard on port.
Command Default	**spanning-tree**	Enabled
	costNumber	2000
	edge-port	None
	point-to-point-mac	**force**

Examples

```
#show running-config
#configure
(config) #interface port-channel 3800
(config-if 3800) #no spanning-tree bpduguard enable
(config-if 3800) #no spanning-tree edge-port
(config-if 3800) #no spanning-tree edge-port auto
(config-if 3800) #no spanning-tree enable
(config-if 3800) #no spanning-tree mac
(config-if 3800) #no spanning-tree mcheck
(config-if 3800) #no spanning-tree point-to-point-mac
(config-if 3800) #no spanning-tree portfast
(config-if 3800) #no spanning-tree rootguard
(config-if 3800) #spanning-tree cost 1000
(config-if 3800) #spanning-tree edge-port auto
(config-if 3800) #spanning-tree mac
(config-if 3800) #spanning-tree mcheck
(config-if 3800) #spanning-tree point-to-point-mac not-force
(config-if 3800) #spanning-tree priority 1
(config-if 3800) #spanning-tree enable
(config-if 3800) #spanning-tree bpduguard enable
(config-if 3800) #spanning-tree portfast
(config-if 3800) #spanning-tree rootguard
```

Revision 1.2

Related Commands `show running-config`

spanning-tree mst

Defines the Multiple Spanning Tree (MST) configuration parameters for a port. BDPUs are used to exchange information about bridge IDs and root path costs.

Command Syntax

spanning-tree mst <*mstInstance*> {**bpduguard enable** | **{{external | internal} cost** <*costNumber*>**}** | **edge-port** [**auto**] | **enable** | **mac** | **mcheck** | **point-to-point-mac** {**force** | **not-force** | **auto**} | **portfast | priority** <*portPriorityNumber*> | **restricted-role** | **restricted-tcn | rootguard**}

no spanning-tree mst <*mstInstance*> {**bpduguard enable** | **edge-port** [**auto**] | **enable** | **mac** | **mcheck** | **point-to-point-mac | portfast | restricted-role** | **restricted-tcn | rootguard** }

Command Modes

Port Channel Interface Configuration Mode

```
#configure
(config) #interface port-channel
portChannel
(config-if) #
```

Syntax Description

bpduguard enable	
mstInstance	MST instance number. The range is 1 to 4094.
external	Configures MST instance external port cost.
internal	Configures MST instance internal port cost.
cost	Sets MST instance port cost.
costNumber	Configures the cost for an interface that is an access port. If a loop occurs, MST considers the path cost when selecting an interface. The range is 1 to 200,000,000. A lower path cost represents a higher transmission speed.
edge-port	Enables edge-port operation to transition directly to the forwarding state. Use the **auto** option to enable automatic discovery of the edge ports.
enable	Enables the MST on the port interface.
mac	Specifies the port as MAC enabled.
mcheck	Enables the port to send Rapid Spanning Tree (RST) BPDUs.
point-to-point-mac	Configures the type of device connected to the port. **force** indicates a point-to-point link to a device such as a switch, bridge, or end-node. **not-force** indicates a connection to a hub which is a shared LAN segment. **auto** causes the switch to set Force-False on the port if it is not running at full duplex.
priority	Configures MST instance port priority.
priorityNumber	Spanning tree priority. The range is 0 to 15.

portfast	Enables or disables PortFast on port.
restricted-role	Enables the restricted role of the port. This parameter prevents the port from becoming a root port.
restricted-tcn	Enables the restricted Topology Change Notification (TCN). This mode does not allow TCN BPDUs to be processed on the port.
rootguard	Enables or disables Root Guard on port.

Command Default **spanning-tree** Enabled

Examples

```
Switch #vlan-database
Switch (vlan)#vlan 10
Switch (config)#spanning-tree mst configuration
Switch (config-mst)#instance 10 vlan 10
#show spanning-tree
#show spanning-tree mst
#show running-config
#configure
(config) #interface port-channel 3800
(config-if 3800) #no spanning-tree mst 10 bpduguard enable
(config-if 3800) #no spanning-tree mst 10 portfast
(config-if 3800) #no spanning-tree mst 10 rootguard
(config-if 3800) #no spanning-tree mst 10 edge-port auto
(config-if 3800) #no spanning-tree mst 10 mac
(config-if 3800) #no spanning-tree mst 10 mcheck
(config-if 3800) #no spanning-tree mst 10 point-to-point-mac
(config-if 3800) #no spanning-tree mst 10 restricted-role
(config-if 3800) #no spanning-tree mst 10 restricted-tcn
(config-if 3800) #no spanning-tree mst 10 enable
(config-if 3800) #spanning-tree mst 10 external cost 1000
(config-if 3800) #spanning-tree mst 10 internal cost 1000
(config-if 3800) #spanning-tree mst 10 bpduguard enable
(config-if 3800) #spanning-tree mst 10 portfast
(config-if 3800) #spanning-tree mst 10 rootguard
(config-if 3800) #spanning-tree mst 10 edge-port auto
(config-if 3800) #spanning-tree mst 10 mac
(config-if 3800) #spanning-tree mst 10 mcheck
(config-if 3800) #spanning-tree mst 10 point-to-point-mac
not-force
(config-if 3800) #spanning-tree mst 10 priority 1
(config-if 3800) #spanning-tree mst 10 restricted-role
(config-if 3800) #spanning-tree mst 10 restricted-tcn
(config-if 3800) #spanning-tree mst 10 enable
```

Revision 1.2

Related Commands

`show spanning-tree mst`

`show running-config`

`spanning-tree (config)`

`spanning-tree mst configuration (mode)`

switchport (config-if, port-channel)

Sets the switching mode parameters for a port. The switchport parameters relate to packet discard mode, 802.1q tunneling (QinQ), ingress filtering, port priority, and port VLANs.
802.1q tunneling allows service providers to use a single VLAN to support multiple customer VLANs while preserving customer VLAN identifiers and segregating customer VLAN traffic.
To view the current configuration of the discard mode, ingress filtering, port default VLAN, and port default priority for all ports, use the **show interface** command.
To view the 802.1q tunneling and port VLAN assignments, use the **show running-config** command.

Command Syntax	**switchport** {**discard** {**all** | **tagged** |**untagged**} | **dot1qtunnel** {**{customer-stacked | customer-mapped [tpid customer]} | {provider-mapped | provider-stacked [tpid {customer | qinq | service}]}**} | **ingress-filtering** | **pvid** <*vlanNumber*>| **pvpt** <*portPriority*>| **vlan {add** <*vlanNumbers*> **tagged|untagged**} | {**mapping** <*customerVlanNumber*> <*customerPortPriority*> <*providerVlanNumber*> <*providerPortPriority*>} } **no switchport** {**discard** | **dot1qtunnel** | **pvid** | **pvpt** | **vlan {add** <*vlanNumbers*> | **mapping** <*customerVlanNumber*> <*customerPortPriority*> <*providerVlanNumber*> <*providerPortPriority*>}}	

Command Modes	Port Channel Interface Configuration Mode	`#configure`
		`(config) #interface port-channel`
		`portChannel (config-if) #`

Syntax Description	**all**	Discards all packets for the port.
	tagged	Discards all VLAN-tagged packets for the port.
	untagged	Discards all untagged packets for the port.
	customer-stacked	Configures interface as customer stacked tunnel.
	customer-mapped	Configures interface as customer mapped tunnel.
	provider-mapped	Configures interface as provider mapped tunnel.
	provider-stacked	Configures interface as provider stacked tunnel.
	tpid customer	Marks frames with Customer VLAN Tag, TPID: 0x8100.
	ingress-filtering	When ingress filtering is disabled, the port accepts any VLAN-tagged frame. When ingress filtering is enabled, incoming frames tagged for VLANs which do not include the ingress port are discarded.
	pvid *vlanNumber*	Specifies the default VLAN identifier for the port. The range is 1 to 4094.
	pvpt *portPriority*	Specifies the default VLAN priority for the port. The range is 0 to 15.
	vlan add *vlanNumbers*	Assigns one or more VLANs to the port. The range is 1 to 4094. Use commas to separate individual values and use dashes to list a range of contiguous VLANs.
	tagged	Supports tagged frames on interface.
	untagged	Supports untagged frames on interface.
Command Default	**discard**	None all for all ports.

dot1qtunnel	None for all ports.
ingress-filtering	None for all ports.
pvid	VLAN 1 untagged for all ports.
pvpt	Priority 0 for all ports.

Examples

```
#show running-config
#configure
(config) #interface port-channel 3800
(config-if 3800) #switchport discard untagged
(config-if 3800) #switchport dot1qtunnel customer-mapped
tpid customer
(config-if 3800) #switchport dot1qtunnel customer-stacked
tpid customer
(config-if 3800) #switchport dot1qtunnel provider-mapped
tpid customer
(config-if 3800) #switchport dot1qtunnel provider-mapped
tpid qinq
(config-if 3800) #switchport dot1qtunnel provider-mapped
tpid service
(config-if 3800) #switchport ingress-filtering
(config-if 3800) #switchport vlan add 2,4,100-102 tagged
(config-if 3800) #switchport vlan add 2,4,100-102 untagged
(config-if 3800) #switchport vlan mapping 1 1 1 1
(config-if 3800) #switchport pvid 2
(config-if 3800) #switchport pvpt 1
 (config-if 3800) #no switchport discard
(config-if 3800) #no switchport ingress-filtering
(config-if 3800) #no switchport pvid
(config-if 3800) #no switchport pvpt
 (config-if 3800) #no switchport vlan add 2,4,100-102
(config-if 3800) #no switchport vlan mapping 1 1 1 1
```

Revision 1.2

Related Commands

`show interface (User)`
`show interface (Privileged)`
`show running-config`
`switchport (config-if interface)`

ufd group

Adds an interface to UFd group.

Command Syntax **[no] ufd group <*groupId*> {ltm | ltd}**

Command Modes

Port Channel Interface Configuration Mode	`#configure` `(config) #interface port-channel` *`portChannel`* `(config-if) #`
group	Adds an interface to UFD group.

groupId	Integer value that uniquely represents the group.
ltm	Adds link to monitor interface to the specific UFD group.
ltd	Adds link to disable interface to the specific UFD group.

Command Default

Examples

```
(config-if 3800)#ufd group 1 ltm
(config-if 3800)#ufd group 1 ltd
(config-if 3800)#no ufd group 1 ltm
(config-if 3800)#no ufd group 1 ltd
```

Revision 1.2

Related Commands `show ufd`

6.7 STP Configuration Mode Commands

instance

Configures the bridge priority of an MST instance. The maximum number of allowed working instances is 255.

Command Syntax [**no**] **instance** <*mstInstance*> {**priority** < *priority*> | **vlan** <*vlanId*> }

Command Modes STP Configuration Mode

```
#configure
(config) #spanning-tree mst
configuration
(config-mst) #
```

Syntax Description

mstInstance	MST instance identifier. The range is 0 to 4094.
priority	Bridge priority. The range is 0 to 61,440.
vlanId	VLAN identifier. The range is 1 to 4094.

Command Default

vlanId	None.

Examples

```
#configure
(config)#spanning-tree mst configuration
(config-mst)#instance 15 priority 12288
(config-mst)#instance 15 vlan 12
(config-mst)#no instance 15 priority
(config-mst)#no instance 15 vlan 12
```

Revision 1.0.1

Related Commands `show spanning-tree mst`

name (config-mst)

Sets the name of the MST configuration.

Command Syntax **name** <*name*>

Command Modes STP Configuration Mode

```
#configure
(config) #spanning-tree mst
configuration
(config-mst) #
```

Syntax Description

name	Name of the MST configuration enclosed in double quotation marks. Enter 1 to 32 characters plus the quotation marks. For example “3”.

Command Default

name	TBD

Examples

```
#show spanning-tree mst configuration
#configure
(config)#spanning-tree mst configuration
```

```
(config-mst)#name “My MST Configuration”
```

Revision 1.0.1

Related Commands `show spanning-tree mst`

revision

Specifies the revision number of the spanning-tree configuration.

Command Syntax **revision** <*revision*>

Command Modes STP Configuration Mode

```
#configure
(config) #spanning-tree mst
configuration
(config-mst) #
```

Syntax Description	*revision*	Revision number of the configuration. The range is 0 to 4095.
Command Default	*revision*	None

Examples

```
#show spanning-tree mst configuration
#configure
(config)#spanning-tree mst configuration
(config-mst)#revision 17
```

Revision 1.0.1

Related Commands

`show spanning-tree mst`

6.8 VLAN Simple Configuration Mode Commands

name (vlan simple)

Assigns a name to a VLAN. The no form of the command is used to set VLAN default name.

Command Syntax	[**no**] **name** <*name*>	

Command Modes	VLAN Simple Configuration Mode	`#configure`
		`(config) #vlan vlanId`
		`(if-vlan vlanId) #`

Syntax Description	*name*	Name of the VLAN enclosed in double quotation marks. Enter 1 to 32 characters plus the quotation marks. For example, "1".
Command Default	VLAN 1	**Default VLAN**
	Other VLANs	**VLAN-***vlanId*

Examples

```
#show vlan
#configure
(config) #vlan 2
(if-vlan 2) #name "My VLAN 2"
(if-vlan 2) #no name
```

Revision 1.0.1

Related Commands

`show vlan (Privileged)`

7. Layer 3 Commands

This section covers the network layer (layer 3) commands for the User mode, Privileged mode, and Global Configuration mode.

7.1 User Mode Commands

ping

Sends ICMP echo-request packets to another node on the network.

Command Syntax **ping** <*host*>

Command Modes User Execution Mode #

Syntax Description		
	host	IP address or IP alias of the host to ping.

Examples

```
#ping 10.0.10.1

PING 10.0.10.1 56 bytes of data.
64 byte(s) from 10.0.10.1: icmp_seq=1 ttl=64 time=0 ms
64 byte(s) from 10.0.10.1: icmp_seq=2 ttl=64 time=0 ms
64 byte(s) from 10.0.10.1: icmp_seq=3 ttl=64 time=0 ms
--- 10.0.10.1 ping statistics ---
3 packet(s) transmitted, 3 packet(s) received
```

Revision 1.0.1

Related Commands

ping6

Sends IPv6 ICMP echo-request packets to another node on the network.

Command Syntax **ping6** <*host*>|<*ipv6Address*>

Command Modes Privileged Mode #

Syntax Description		
	host	IP address or IP alias of the host to ping.
	ipv6Address	IPv6 address of the host to ping.

Examples

```
#ping6 10.0.10.1

PING 10.0.10.1 (10.0.10.1) 56(84) bytes of data.

--- 10.0.10.1 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time
2999ms
```

```
#ping6 128.224.187.151

PING 128.224.187.151 (128.224.187.151) 56(84) bytes of data.
64 bytes from 128.224.187.151: icmp_req=1 ttl=60 time=74.9
ms
64 bytes from 128.224.187.151: icmp_req=2 ttl=60 time=73.9
ms
64 bytes from 128.224.187.151: icmp_req=3 ttl=60 time=73.9
ms
64 bytes from 128.224.187.151: icmp_req=4 ttl=60 time=73.9
ms

--- 128.224.187.151 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time
3008ms
rtt min/avg/max/mdev = 73.989/74.239/74.989/0.433 ms
```

Revision 1.2

Related Commands

7.2 Privileged Mode Commands

ping

Sends ICMP echo-request packets to another node on the network.

Command Syntax	**ping** *<host>*|*<ipv4Address>*	
Command Modes	Privileged Mode	#
Syntax Description	*host*	IP address or IP alias of the host to ping.
	ipv4Address	IPv4 address of the host to ping.

Examples

```
#ping 10.0.10.1

PING 10.0.10.1 56 bytes of data.
64 byte(s) from 10.0.10.1: icmp_seq=1 ttl=64 time=0 ms
64 byte(s) from 10.0.10.1: icmp_seq=2 ttl=64 time=0 ms
64 byte(s) from 10.0.10.1: icmp_seq=3 ttl=64 time=0 ms
--- 10.0.10.1 ping statistics ---
3 packet(s) transmitted, 3 packet(s) received

#ping 128.224.187.151

PING 128.224.187.151 (128.224.187.151) 56(84) bytes of data.
64 bytes from 128.224.187.151: icmp_req=1 ttl=60 time=74.9
ms
64 bytes from 128.224.187.151: icmp_req=2 ttl=60 time=75.9
ms
64 bytes from 128.224.187.151: icmp_req=3 ttl=60 time=73.9
ms
64 bytes from 128.224.187.151: icmp_req=4 ttl=60 time=73.9
ms

--- 128.224.187.151 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time
3008ms
rtt min/avg/max/mdev = 73.988/74.738/75.989/0.873 ms
```

Revision 1.2

Related Commands

ping6

Sends IPv6 ICMP echo-request packets to another node on the network.

Command Syntax **ping6** *<host>*|*<ipv6Address>*

Command Modes	Privileged Mode	#
Syntax Description	*host*	IP address or IP alias of the host to ping.
	ipv6Address	IPv6 address of the host to ping.

Examples

```
#ping6 10.0.10.1

PING 10.0.10.1 (10.0.10.1) 56(84) bytes of data.

--- 10.0.10.1 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time
2999ms

#ping6 128.224.187.151

PING 128.224.187.151 (128.224.187.151) 56(84) bytes of data.
64 bytes from 128.224.187.151: icmp_req=1 ttl=60 time=74.9
ms
64 bytes from 128.224.187.151: icmp_req=2 ttl=60 time=73.9
ms
64 bytes from 128.224.187.151: icmp_req=3 ttl=60 time=73.9
ms
64 bytes from 128.224.187.151: icmp_req=4 ttl=60 time=73.9
ms

--- 128.224.187.151 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time
3008ms
rtt min/avg/max/mdev = 73.989/74.239/74.989/0.433 ms
```

Revision 1.2

Related Commands

show ip igmp snooping

Shows IP IGMP configuration.

Command Syntax **show ip igmp snooping [interface [<*interfaceId*> | {port-channel <*portChannel*>}] [stats | mrouter | {groups [static]}]]**

Command Modes	Privileged Mode	#
Syntax Description	**igmp**	Shows IP IGMP configuration.
	snooping	Shows global IP IGMP snooping configuration.
	interface	Shows IP IGMP information per interface.
	interfaceId	Specifies interface name to show information for.

port-channel	Shows IP IGMP information per port-channel.
portChannel	Port-channel number to show information for.
stats	Shows IP IGMP statistics information per interface.
mrouter	Shows information an all router ports on the device.
groups	Shows information of all VLAN/multicast groups on the device.
static	Shows information about static multicast entries.
vlanNumber	Shows IGMP snooping information for specified VLAN.
macAddress	Shows IGMP snooping information for specified MAC address.

Command Default

This command has no default settings.

Examples

```
#show ip igmp snooping#show ip igmp snooping interface
#show ip igmp snooping interface xe1
#show ip igmp snooping interface xe1 stats
#show ip igmp snooping interface xe1 mrouter
#show ip igmp snooping interface xe1 groups
#show ip igmp snooping interface xe1 groups static
#show ip igmp snooping interface stats
#show ip igmp snooping interface mrouter
#show ip igmp snooping interface groups
#show ip igmp snooping interface groups static
#show ip igmp snooping interface port-channel 3800
#show ip igmp snooping interface port-channel 3800 stats
#show ip igmp snooping interface port-channel 3800 mrouter
#show ip igmp snooping interface port-channel 3800 groups
#show ip igmp snooping interface port-channel 3800 groups
static
```

System Response

The output fields for **snooping** are as follows:

Field	Description
IP IGMP Status	Shows Routing Admin Status.
Router Port Administrative Status	Enabled or Disabled Routing Admin Status.
Router Port Operational Mode	Shows the multicast router port status of this port.
Host Port	Shows the multicast host port status of this port.
RX IGMP v1 Queries	Displays the number of V1 IGMP Queries received on this port.
RX IGMP v2 Queries	Displays the number of V2 IGMP Queries received on this port.
RX IGMP v3 Queries	Displays the number of V3 IGMP Queries received on this port.
RX IGMP v1 Reports	Displays the number of V1 IGMP Reports received on this port.
RX IGMP v2 Reports	Displays the number of V2 IGMP Reports received on this port.
RX IGMP v3 Reports	Displays the number of V3 IGMP Reports received on this port.
RX IGMP Leaves	Displays the number of IGMP Leaves received on this port.

Number Of Groups	Shows the number of groups this port has subscribed to.
VLAN	VLAN ID.
Group MAC Address	Shows IGMP snooping group MAC address.
Interface	Interface ID.
IP IGMP Status	Shows Routing Admin Status.
Router Port	Shows the multicast router port status of this port.
Host Port	Shows the multicast host port status of this port.

The output fields for **snooping interface** are as follows:

Field	Field
Interface	Interface ID.
IP IGMP Status	Shows Routing Admin Status.
Router Port Administrative Status	Enabled or Disabled Routing Admin Status.
Router Port Operational Mode	Shows the multicast router port status of this port.
Host Port	Shows the multicast host port status of this port.
RX IGMP v1 Queries	Displays the number of V1 IGMP Queries received on this port.
RX IGMP v2 Queries	Displays the number of V2 IGMP Queries received on this port.
RX IGMP v3 Queries	Displays the number of V3 IGMP Queries received on this port.
RX IGMP v1 Reports	Displays the number of V1 IGMP Reports received on this port.
RX IGMP v2 Reports	Displays the number of V2 IGMP Reports received on this port.
RX IGMP v3 Reports	Displays the number of V3 IGMP Reports received on this port.
RX IGMP Leaves	Displays the number of IGMP Leaves received on this port.
Number Of Groups	Shows the number of groups this port has subscribed to.
VLAN	VLAN ID.
Group MAC Address	Shows IGMP snooping group MAC address.

The output fields for **snooping interface groups** are as follows:

Field	Field
Number of Groups	Shows the number of groups this port has subscribed to.
VLAN	VLAN ID.
Interface	Interface ID.
Group MAC Address	Shows IGMP snooping group MAC address.
Group Type	Shows IGMP snooping group type.

The output fields for **snooping interface xe1 groups** are as follows:

Field	Field
Number of Groups	Shows the number of groups this port has subscribed to.
VLAN	VLAN ID.
Interface	Interface ID.
Group MAC Address	Shows IGMP snooping group MAC address.
Group Type	Shows IGMP snooping group type.

The output fields for **snooping interface groups static** are as follows:

Field	Field

Number of Groups	Shows the number of groups this port has subscribed to.
VLAN	VLAN ID.
Interface	Interface ID.
Group MAC Address	Shows IGMP snooping group MAC address.

The output fields for **snooping interface xe1 groups static** are as follows:

Field	Field
Number of Groups	Shows the number of groups this port has subscribed to.
VLAN	VLAN ID.
Interface	Interface ID.
Group MAC Address	Shows IGMP snooping group MAC address.

The output fields for **snooping interface mrouter** are as follows:

Field	Field
Number Of Routers	Shows number of multicast routers.
Interface	Interface ID.
RX IGMP v1 Queries	Displays the number of V1 IGMP Queries received on this port.
RX IGMP v2 Queries	Displays the number of V2 IGMP Queries received on this port.
RX IGMP v3 Queries	Displays the number of V3 IGMP Queries received on this port.

The output fields for **snooping interface xe1 mrouter** are as follows:

Field	Field
Number Of Routers	Shows number of multicast routers.
Interface	Interface ID.
RX IGMP v1 Queries	Displays the number of V1 IGMP Queries received on this port.
RX IGMP v2 Queries	Displays the number of V2 IGMP Queries received on this port.
RX IGMP v3 Queries	Displays the number of V3 IGMP Queries received on this port.

The output fields for **snooping interface stats** are as follows:

Field	Field
Interface	Interface ID.
RX IGMP v1 Queries	Displays the number of V1 IGMP Queries received on this port.
RX IGMP v2 Queries	Displays the number of V2 IGMP Queries received on this port.
RX IGMP v3 Queries	Displays the number of V3 IGMP Queries received on this port.
RX IGMP v1 Reports	Displays the number of V1 IGMP Reports received on this port.
RX IGMP v2 Reports	Displays the number of V2 IGMP Reports received on this port.
RX IGMP v3 Reports	Displays the number of V3 IGMP Reports received on this port.
RX IGMP Leaves	Displays the number of IGMP Leaves received on this port.

Revision 1.1

Related Commands

`ip igmp snooping`

show ip name-server

Shows information about configured name servers.

Command Syntax **show ip name-server**

Command Modes Privileged Mode #

Command Default This command has no default settings.

Examples

```
#show ip name-server
```

System Response The output fields for **name-server** are as follows:

Field	Description
Name Server IP Address	IP Address of the configured name server.
Search Prefix	DNS search prefix.

Revision 1.0.1

Related Commands