FAB10Gxxxx
FAB40Gxxxx

Firmware Revision Level: 42XX_8.10-xx
Contents

CHAPTER 1: INTRODUCTION ........................................................................................................... 5
  1.1 PURPOSE ............................................................................................................................ 5
  1.2 SCOPE ............................................................................................................................... 5
  1.3 DOCUMENT CONVENTIONS .............................................................................................. 5
  1.4 KEYBOARD CONVENTIONS ............................................................................................. 6

CHAPTER 2: COMMAND LINE INTERFACE ............................................................................... 7
  2.1 CLI COMMAND Modes .......................................................................................................... 8
  2.2 USER EXEC Mode ................................................................................................................ 9
  2.3 PRIVILEGED EXEC Mode ..................................................................................................... 9
  2.4 GLOBAL CONFIGURATION Mode ....................................................................................... 9
  2.5 INTERFACE CONFIGURATION Mode .................................................................................. 9
  2.6 CONFIG-VLAN Mode .......................................................................................................... 9
  2.7 LINE CONFIGURATION Mode ........................................................................................... 9

CHAPTER 3: LINK AGGREGATION ............................................................................................... 11
  3.1 SHOW ETHERCHANNEL ...................................................................................................... 11
  3.2 SHOW INTERFACES ........................................................................................................... 13

CHAPTER 4: SSH AND TELNET ............................................................................................... 15
  4.1 IP SSH ............................................................................................................................... 15
  4.2 SSH .................................................................................................................................. 16
  4.3 SHOW IP SSH .................................................................................................................... 17
  4.4 SET TELNET ..................................................................................................................... 17

CHAPTER 5: PORT MIRRORING ................................................................................................. 18
  5.1 MONITOR SESSION SOURCE ............................................................................................ 18
  5.2 MONITOR SESSION DESTINATION ................................................................................... 19

CHAPTER 6: FAB TRAFFIC FLOW CONFIGURATION ............................................................... 20
  6.1 SYSTEM OVERVIEW .......................................................................................................... 20
  6.2 CONFIGURATION MAPS .................................................................................................... 20
  6.3 PORT CHANNEL ................................................................................................................ 23
  6.4 VIRTUAL TRUNK ............................................................................................................... 24
  6.5 FILTER TEMPLATES .......................................................................................................... 26
  6.6 SWAP-PRIORITY CFG-MAP1 CFG-MAP2 ......................................................................... 41
  6.7 SET FILTER-MATCH POLL-TIME-INTERVAL ................................................................. 41
  6.8 SET TAGGING-MODE ........................................................................................................ 41
  6.9 SET HASH-MODE .............................................................................................................. 42
  6.10 SET L2-VPN-MPLS-STRIP ............................................................................................. 42
  6.11 SET NAME ...................................................................................................................... 42
  6.12 SET DESCRIPTION ........................................................................................................... 43
  6.13 SET NESTED-VLAN .......................................................................................................... 43
  6.14 SET IN-TRAFFIC .............................................................................................................. 43
  6.15 SET OUT-TRAFFIC .......................................................................................................... 43
  6.16 SET CRC-HASH .............................................................................................................. 44
  6.17 SET LINK-MODE ............................................................................................................. 45
  6.18 SHOW PORT MPLS-STRIP-DETAILS .............................................................................. 45
  6.19 SHOW PORT NAME .......................................................................................................... 45
  6.20 SHOW PORT DESCRIPTION ............................................................................................. 46
  6.21 SHOW TAGGING-MODE .................................................................................................. 46
  6.22 SHOW NESTED-VLAN INFO ........................................................................................... 47
<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.23</td>
<td>SHOW IN-TRAFFIC INFO</td>
</tr>
<tr>
<td>6.24</td>
<td>SHOW OUT-TRAFFIC INFO</td>
</tr>
<tr>
<td>6.25</td>
<td>SHOW GLOBAL HASH-MODE</td>
</tr>
<tr>
<td>6.26</td>
<td>SHOW CRC-HASH-POLICY</td>
</tr>
<tr>
<td>6.27</td>
<td>SHOW HASH-MODE-INFO</td>
</tr>
<tr>
<td>6.28</td>
<td>SHOW LINK-MODE INFO</td>
</tr>
<tr>
<td>6.29</td>
<td>SHOW FILTER-MATCH POLL-TIME-INTERVAL</td>
</tr>
<tr>
<td>6.30</td>
<td>SHOW FILTER-MATCH COUNT</td>
</tr>
<tr>
<td>6.31</td>
<td>CLEAR FILTER-MATCH</td>
</tr>
<tr>
<td>6.32</td>
<td>SHOW PORT-GROUP</td>
</tr>
<tr>
<td>6.33</td>
<td>SHOW CONFIGURATION MAP</td>
</tr>
<tr>
<td>6.34</td>
<td>SHOW ACCESS-LISTS</td>
</tr>
</tbody>
</table>

**CHAPTER 7: FAB PORT SECURITY**

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>Security Configuration Overview</td>
</tr>
<tr>
<td>7.2</td>
<td>ADD USER</td>
</tr>
<tr>
<td>7.3</td>
<td>SET USER</td>
</tr>
<tr>
<td>7.4</td>
<td>NO USER</td>
</tr>
<tr>
<td>7.5</td>
<td>SHOW USER</td>
</tr>
<tr>
<td>7.6</td>
<td>ADD GROUP</td>
</tr>
</tbody>
</table>

**CHAPTER 8: FAB PORT SPEED**

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Port Speed Configuration Overview</td>
</tr>
<tr>
<td>8.2</td>
<td>SET FORCE-SPEED</td>
</tr>
<tr>
<td>8.3</td>
<td>SHOW PORT FORCE-SPEED</td>
</tr>
<tr>
<td>8.4</td>
<td>SHOW PORT SFP</td>
</tr>
</tbody>
</table>
1. Introduction

1.1 Purpose
This document describes in detail the CLI commands that are specific to the Garland Technology FAB. It is intended to be a reference manual for users and system administrators who will configure the Garland Technology FAB through the CLI interface.

1.2 Scope
The scope of this document is limited to the Garland Technology FAB release 5.0.0.0. This document details all the CLI based commands provided by the Garland Technology FAB software.

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

Keyboard shortcuts

<table>
<thead>
<tr>
<th>Key Combination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up Arrow / Down Arrow</td>
<td>Displays the previously executed command</td>
</tr>
<tr>
<td>Ctrl + C</td>
<td>Exits from the SWITCH prompt</td>
</tr>
<tr>
<td>Backspace / Ctrl + H</td>
<td>Removes a single character</td>
</tr>
<tr>
<td>TAB</td>
<td>Completes a command without typing the full word</td>
</tr>
<tr>
<td>Left Arrow / Right Arrow</td>
<td>Traverses the current line</td>
</tr>
</tbody>
</table>

Others

- `?` - helps to list the available commands
- `'q` - exits the output display if display is more than one page and returns to the SWITCH prompt
- "show history" - displays the command history list
Chapter 2

2. Command Line Interface

This section describes the configuration of the Garland Technology FAB using the Command Line Interface.

The Command Line Interface (CLI) can be used to configure the Garland Technology FAB from a console attached to the serial port of the switch or from a remote terminal using TELNET or SSH.

The Garland Technology FAB CLI supports a simple login authentication mechanism. The authentication is based on a user name and password provided by the user during login. The user "root" is created by default with password "gtroot1".

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

Garland Technology FAB Switch Solution
Switch# Login: root
Password: ********
Switch#

The "user-exec" mode is now available to the user. CLI Command Modes provide a detailed description of the various modes available for FAB.

The command prompt always displays the current mode.

- CLI commands need not be fully typed. The abbreviated forms of CLI commands are also accepted by the Garland Technology FAB CLI. For example, commands like "show ip global config" can be typed as "sh ip gl co".
- CLI commands are case insensitive.
- CLI commands will be successful only if the dependencies are satisfied for a particular command that is issued. Appropriate error messages will be displayed, if the dependencies are not satisfied.

Note: The ethernet type of an interface is determined during System Startup. While configuring interface-specific parameters, its ethernet type needs to be specified correctly. A fast ethernet interface cannot be configured as a gigabit ethernet interface and vice-versa.
### 2.1 CLI Command Modes

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit method</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC</td>
<td>This is the initial mode to start a session.</td>
<td>Switch&gt;</td>
<td>The logout method is used.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>The User EXEC mode command enable, is used to enter the Privileged EXEC mode.</td>
<td>Switch#</td>
<td>To return from the Privileged EXEC mode to User EXEC mode the disable command is used.</td>
</tr>
<tr>
<td>Global Configuration</td>
<td>The Privileged EXEC mode command configure terminal, is used to enter the Global Configuration mode.</td>
<td>Switch(config)#</td>
<td>To exit to the Global Configuration mode the exit command is used and to exit to the Privileged EXEC mode the end command is used.</td>
</tr>
<tr>
<td>Interface Configuration</td>
<td>The Global Configuration mode command interface &lt;interface-type&gt;&lt;interface-id&gt; is used to enter the Interface configuration mode.</td>
<td>Switch(config-if)#</td>
<td>To exit to the Global Configuration mode the exit command is used and to exit to the Privileged EXEC mode the end command is used.</td>
</tr>
<tr>
<td>Config-VLAN</td>
<td>The global configuration mode command vlan vlan-id, is used to enter the Config-VLAN mode.</td>
<td>Switch(config-vlan)#</td>
<td>To exit to the Global Configuration mode the exit command is used and to exit to the Privileged EXEC mode the end command is used.</td>
</tr>
<tr>
<td>Line Configuration</td>
<td>The global configuration mode command line, is used to enter the Line Configuration mode.</td>
<td>Switch(config-line)#</td>
<td>To exit to the Global Configuration mode the exit command is used and to exit to the Privileged EXEC mode the end command is used.</td>
</tr>
</tbody>
</table>
2.2 User EXEC Mode
If logging into the device with a username other than ‘root’, the user is automatically placed in the User EXEC mode. In general, the User EXEC commands are used to temporarily change terminal settings, perform basic tests and list system information.

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

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

2.5 Interface Configuration Mode
The Interface Configuration mode allows for configuration of Physical Interfaces, Port Channels, and VLAN’s. The Physical Interface mode is used to perform interface specific operations. Port Channel Interface mode is used to perform port-channel specific operations. VLAN Interface mode is used to perform L3-IPVLAN specific operations. To return to the global configuration mode from any of these configuration modes the exit command is used.

2.6 Config-VLAN Mode
This mode is used to perform VLAN specific operations. To return to the global configuration mode the exit command is used.

2.7 Line Configuration Mode
Line configuration commands modify the operations of a terminal line.
User EXEC Mode
Prompt: switch> enable

Password

Privileged Mode
Prompt: switch#

Global Configuration Mode
Prompt: switch(config)#

Protocol Specific Modes

- DHCP Pool Configuration
  Prompt: switch(dhcp-config)#

- ACL Standard Access List Configuration
  Prompt: switch(config-std-nacl)#

- ACL Extended Access List Configuration
  Prompt: switch(config-ext-nacl)#

- ACL MAC Configuration
  Prompt: switch(config-ext-macl)#

General Configuration Modes

- Line Configuration
  Prompt: switch(config-line)#

- Interface Configuration Mode
  Prompt: switch(config-if)#

- Config-VLAN
  Prompt: switch(config-vlan)#

Figure 2-1: Command Modes Access Path
3. Link Aggregation

LA (Link Aggregation) is a method of combining physical network links into a single logical link for increased bandwidth. LA increases the capacity and availability of the communications channel between devices (both switches and end stations) using existing Fast Ethernet and Gigabit Ethernet technology. LA also provides load balancing where the processing and communication activity is distributed across several links in a trunk, so that no single link is overwhelmed. By taking multiple LAN connections and treating them as a unified, aggregated link, practical benefits in many applications can be achieved. LA provides the following important benefits:

- Higher link availability
- Increased link capacity
- Improvements are obtained using existing hardware (no upgrading to higher-capacity link technology is necessary)

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

- show etherchannel
- show interfaces

3.1 show etherchannel

This command displays EtherChannel information.

`show etherchannel [[channel-group-number] [ detail | load-balance | port | port-channel | summary | protocol]]`

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-group-number</td>
<td>Number of the channel group. Valid numbers range from maximum number of ports in the system to maximum number of aggregations supported</td>
</tr>
<tr>
<td>detail</td>
<td>Detailed EtherChannel information</td>
</tr>
<tr>
<td>load-balance</td>
<td>Load-balance or frame-distribution scheme among ports in the port channel</td>
</tr>
<tr>
<td>port</td>
<td>EtherChannel port information</td>
</tr>
</tbody>
</table>
port-channel - Port-channel information
summary - Protocol that is being used in the EtherChannel
protocol - One-line summary per channel-group

Mode
Privileged EXEC Mode

Example
Switch# show etherchannel 1 detail
Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel System Identifier is 00:01:02:03:04:01
LACP System Priority: 32768

Channel Group Listing
---------------------
Group: 1
----------
Protocol :LACP

Ports in the Group
---------------------
Port :Ex 0/1
----------
Port State = Up in Bundle
Channel Group : 1
Mode : Active
Pseudo port-channel = Po1
LACP port-priority = 128
LACP Wait-time = 2 secs
LACP Activity : Active
LACP Timeout : Long

Aggregation State : Aggregation, Sync, Collecting, Distributing, Defaulted

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Priority</th>
<th>Key</th>
<th>Key Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ex0/1</td>
<td>Bundle</td>
<td>128</td>
<td>1</td>
<td>0x1</td>
<td>0xbe</td>
</tr>
</tbody>
</table>

Port-channel : Po1

Number of Ports = 1
HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = LACP
Aggregator-MAC 00:01:02:03:04:19
Default Port = None

If the channel group number is not specified, details on all channels are displayed.

Related Commands
- show interfaces – Displays interface specific port-channel information
3.2 show interfaces

This command displays interface specific port-channel information.

```
show interfaces [interface-type] [interface-id] etherchannel
```

**Syntax**

etherchannel - Interface EtherChannel information

**Description**

Privileged EXEC Mode

**Example**

Switch# show interfaces ex 0/1 etherchannel
Port : Ex0/1

<table>
<thead>
<tr>
<th></th>
<th>LACP Port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ex0/1</td>
<td>Bundle</td>
<td>128</td>
<td>2</td>
<td>2</td>
<td>0x1</td>
</tr>
</tbody>
</table>

Switch# show interfaces etherchannel
Port : Ex0/1

Port State = Up in Bundle
Channel Group : 2
Mode : Active
Pseudo port-channel = Po2
LACP port-priority = 128
LACP Port Identifier = 2
LACP Wait-time = 2 secs
LACP Activity : Passive
LACP Timeout : Long

Aggregation State : Aggregation, Sync, Collecting, Distributing,
Pseudo port-channel = Po2
LACP port-priority = 128
LACP Wait-time = 2 secs
LACP Activity : Passive
LACP Timeout : Long

Aggregation State : Aggregation, Sync, Collecting, Distributing,

<table>
<thead>
<tr>
<th>Port</th>
<th>LACP Port</th>
<th>Admin Priority</th>
<th>Oper Priority</th>
<th>Port Key</th>
<th>Port Key</th>
<th>Port Number</th>
<th>Port State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ex0/1</td>
<td>Bundle 128</td>
<td>2</td>
<td>2</td>
<td>0x1</td>
<td>0x3c</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ex0/2</td>
<td>Bundle 128</td>
<td>2</td>
<td>2</td>
<td>0x2</td>
<td>0x3c</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Port-channel : Po2

Number of Ports = 2
HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = LACP
Aggregator-MAC 00:01:02:03:04:23
Default Port = None

- Expressions are case sensitive.
- The port-channel range is 1 to 64.

Related Commands
- show etherchannel - Displays Etherchannel information
4. SSH and TELNET

SSH is a protocol for secure remote login and other secure network services over an insecure network. It consists of three major components:

- The Transport Layer Protocol provides server authentication, confidentiality, and integrity.
- The User Authentication Protocol authenticates the client-side user to the server. It runs over the transport layer protocol.
- The Connection Protocol multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol.

The client sends a service request once a secure transport layer connection has been established. A second service request is sent after user authentication is complete. This allows new protocols to be defined and coexist with these protocols.

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

- `ip ssh`
- `ssh`
- `show ip ssh`
- `set telnet`

4.1 ip ssh

This command enables the SSH server on the device and also configures the various parameters associated with the SSH server. The no form of the command disables the SSH server on the device and also re-sets the various parameters associated with the SSH server.

```
ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth ([hmac-md5] [hmac-shal]) }

no ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth ([hmac-md5] [hmac-shal]) }
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version compatibility</td>
<td>The support for the SSH protocol version</td>
</tr>
</tbody>
</table>

- The support for the SSH protocol version
cipher - The cipher-algorithm list. This includes:
  - des-cbc - Data Encryption Standard - Cipher Block Chaining
  - 3des-cbc – Triple Data Encryption Standard - Cipher Block Chaining

auth - Public key authentication for incoming SSH sessions. This includes:
  - hmac-md5 - Hash Message Authentication Code - Message-Digest algorithm 5
  - hmac-sha1 - Hash Message Authentication Code - Secure Hash Algorithm 1

Mode Global configuration mode false
Defaults version compatibility
cipher - 3des-cbc
auth - hmac-sha1

Example
Switch(config)#ip ssh version compatibility
Switch(config)#ip ssh cipher des-cbc

- When version compatibility is set to TRUE, both SSH version-1 and SSH version-2 will be supported. When set to FALSE, SSH version-2 only will be supported
- The cipher list takes values as bit mask. Setting a bit indicates that the corresponding cipher-list will be used for encryption
- The auth takes values as bit mask. Setting a bit indicates that the corresponding MAC-list will be used for authentication

Related Command
  - show ip ssh - Displays SSH server information

4.2 ssh

This command enables or disables the ssh subsystem.

ssh {enable | disable}

Syntax enable - Enables the ssh subsystem.
   disable - Disables the ssh subsystem.

Mode Global configuration Mode

Example Switch# ssh enable

Related Command
  - ip ssh - Enables an SSH server on the device and configures the various parameters associated with the SSH server
4.3 show ip ssh

This command displays SSH server information.

show ip ssh

Mode: Privileged EXEC Mode

Example

Switch# show ip ssh
Version : 2
Cipher Algorithm : 3DES-CBC
Authentication : HMAC-SHA1
Trace Level : None

Related Command
- ip ssh - Enables the SSH server on the device and configures the various parameters associated with the SSH server

4.4 set telnet

Enables or disables remote Telnet access.

set telnet { enable | disable }

Syntax

description

table

type

Mode: Global Configuration Mode

Example

Switch(config)# set telnet disable
Chapter 5

5. Port Mirroring

Configuring port mirroring will set the device to mirror either all packets received, sent, or both, received and sent to another port on the device. The available configurations are one-to-one or many-to-one mirroring. The system supports up to 7 mirroring configurations. The list of CLI commands for the configuration of Port Mirroring is as follows:

- monitor session source
- monitor session destination

5.1 monitor session source

This command sets the source port(s) for mirroring. This command also sets whether the traffic to be mirrored is transmitted packets (Tx), received packets (Rx), or both (Tx and Rx).

```
monitor session <integer(1-7)> source interface extreme-ethernet <port-id> {tx | rx | both}
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>integer</td>
<td>Specifies the port mirroring configuration to be set.</td>
</tr>
<tr>
<td>source</td>
<td>Sets the specified interface as the source port(s) to be mirrored.</td>
</tr>
<tr>
<td>port-id</td>
<td>The port-ID of the interface to be mirrored.</td>
</tr>
<tr>
<td>tx</td>
<td>Only traffic sent out on the specified port will be mirrored to the destination port.</td>
</tr>
<tr>
<td>rx</td>
<td>Only traffic received on the specified port will be mirrored to the destination port.</td>
</tr>
<tr>
<td>both</td>
<td>All traffic transmitted and received on the specified port will be mirrored to the destination port.</td>
</tr>
</tbody>
</table>
Mode  
Global Configuration Mode

Example  
Switch(config)# monitor session 1 source interface extreme-ethernet 0/1 rx

5.2 monitor session destination

This command sets the destination port for mirroring. There can only be one destination port per port mirror configuration.

```
monitor session <integer(1-7)> destination interface extreme-ethernet <port-id>
```

**Syntax**

**integer**

- Specifies the port mirroring configuration to be set.

**destination**

- Sets the specified interface as the destination port of the mirror.

**port-id**

- The port-ID of the interface to be mirrored to.

**Mode**  
Global Configuration Mode

**Example**  
Switch(config)# monitor session 1 destination interface extreme-ethernet 0/2
Chapter 6

6. FAB Traffic Flow Configuration

The FAB system is capable of doing advanced traffic aggregation, mirroring, ingress and egress filtering, load balancing, packet truncation, tagging and protocol striping.

6.1 System Overview

Traffic flow inside the system is defined based on configuration maps. It has input ports, output ports/portgroups and filters. In the above diagram traffic coming from the network enters into FAB on input port and leaves the device on the output ports connected to servers.

6.2 Configuration Maps

Configuration map defines traffic from set of input ports to set of output ports/portgroups. Following are the CLI commands.

**CLI Command:**

```
Configuration map <id>
```

**Syntax Description:**

Enters into configuration map mode for creating or updating. If id is not specified system will automatically assign id for this configuration map.

**CLI Command:**

```
input-ports [<interface-type> <interface-id>] output-ports [<interface-type> <interface-id>] [port-channel <a,b,c-d>]] [ vtrunk <integer(1-50)> ]
```
Syntax Description:

input-ports - List of input ports belongs to this configuration map.

[<interface-type>] - Type of the input port.
[<interface-id>] - Id for the input port.

output-port - List of output ports for this configuration map.

[<interface-type>] - Type of the output port.
[<interface-id>] - Id for the output port.

[port-channel-id] - Id for output port-channel

[vtrunk <integer(1-50)>] - Id for output virtual trunk

CLI Command:

filter { pass-all | deny-all | template { mac | ip | udb } <integer(1-65535)>}

Syntax Description:

Filter - Specifies filter mode for this configuration map.
Pass-all - Send all the traffic from input to output ports/portgroups.
Deny-all - Deny all the traffic coming from input.
Template - Specify mac or ip or udb filter that for this configuration map.

CLI Command:

advanced-action { strip-vlan | tag-vlan <integer(2-99)> | pkt-truncate | none [<integer(100-4094)>] 13- vpn- mpls- strip [tag-vlan <integer(2-99)>] }

Syntax Description:

Advanced-action - Specifies advanced options for this configuration map.
Strip-vlan - Removes vlan tag present in the packet.
Tag-vlan - Add vlan tag to all the packets with this id.
Pkt-truncate - Truncate the packet and send only the header to Tool device.
None - Do not modify the packet.
Send the packet to output ports without any modification.
13- vpn- mpls- strip - Strip MPLS label from 13- vpn- mpls traffic and forward the passenger packet to output port.
tag-vlan id - After MPLS strip tag the packet with this vlan id.
CLI Command:

```
set name <cfg-map-name>
```

Syntax Description:
Specifies name for the configuration map.

CLI Command:

```
set description <cfg-map-desc>
```

Syntax Description:
Specifies description for the configuration map.

CLI Command:

```
set configuration-map { enable | disable }
```

Syntax Description:
Enable/Disable the configuration map.

CLI Command:

```
no configuration map <id> | all
```

Syntax Description:
Delete specific configuration map if id is specified or delete entire configuration map if all is specified.

CLI Command:

```
show configuration map <id> | all
```

Syntax Description:
Shows specific configuration map if the id is specified or shows all the configuration map if all is specified.

Example:

The following configuration map example shows how to do aggregation using configuration map. Traffic coming from network on input ports 1,2,3,4 and 5 is aggregated to output port 24.

```
Switch(config)# configuration map
Creating New Configuration Map :: 1

Switch(config-map-1)# input-ports extreme-ethernet 0/1-5 output-ports extreme-ethernet 0/24
```
6.3 Port Channel

Many physical ports can be grouped to form a port channel.

**CLI Command:**

```
port-channel <id>
```

**Syntax Description:**

Enters into port-channel mode for creating or updating. If id is not specified system will automatically assign id for this port channel.

**CLI Command:**

```
ports [interface-type] [interface-id]
```

**Syntax Description:**

Assigns multiple physical ports to this port channel.

**CLI Command:**

```
set description <port-channel-desc>
```

**Syntax Description:**

Specifies description for the port channel.

**CLI Command:**

```
No port-channel <id>
```

**Syntax Description:**

Deletes port channel from the system.

**CLI Command:**

```
port-channel load-balance {src-mac | dest-mac | src-dest-mac | src-ip | dest-ip | src-dest-ip | mpls-vc-label | mpls-tunnel-label | mpls-vc-tunnel-label}
```

**Syntax Description**

* src-mac - Load distribution is based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port
dest-mac - Load distribution is based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.

src-dest-mac - Load distribution is based on the source and destination MAC address.

src-ip - Load distribution is based on the source IP address.

dest-ip - Load distribution is based on the destination IP address.

src-dest-ip - Load distribution is based on the source and destination IP address.

mpls-vc-label - Link selection policy is based on MPLS VC label.

mpls-tunnel-label - Link selection policy is based on MPLS tunnel label.

mpls-vc-tunnel-label - Link selection policy is based on the combination of MPLS VC and tunnel label.

Example:

The following example creates and add port 20,21,22 and 23 to port channel.

```
Switch(config)# port-channel
Creating New Port Channel :: 25

Switch(config-port-channel-25)# ports extreme-ethernet 0/20-23
```

This port channel can be assigned to an output of configuration map. For example 10G traffic coming from the network on input ports 1 and 2 can be load balanced to port channel 25.

```
Switch(config)# configuration map
Creating New Configuration Map :: 1

Switch(config-map-1)# input-ports extreme-ethernet 0/1,0/2 output-ports port-channel 25
```

6.4 Virtual Trunk

Many physical ports can be grouped to form virtual trunk. It similar to port channel but it can contain any number of port channels and flexible load balancing policy.

CLI Command:

```
Virtual-trunk <id>
```

Syntax Description:

Enters into virtual trunk mode for creating or updating. If id is not specified system will automatically assign id for this virtual trunk.
CLI Command:

```
ports [interface-type] [interface-id]
```

Syntax Description:
Assigns multiple physical ports to this virtual trunk.

CLI Command:

```
set description <virtual-trunk-desc>
```

Syntax Description:
Specifies description for the virtual trunk.

CLI Command:

```
No virtual-trunk <id>
```

Syntax Description:
Deletes virtual trunk from the system.

CLI Command:

**Syntax Description**

- `src-mac`
  - Load distribution is based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.

- `dest-mac`
  - Load distribution is based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.

- `src-dest-mac`
  - Load distribution is based on the source and destination MAC address.

- `src-ip`
  - Load distribution is based on the source IP address.

- `dest-ip`
  - Load distribution is based on the destination IP address.

- `src-dest-ip`
  - Load distribution is based on the source and destination IP address.

- `mpls-vc-label`
  - Link selection policy is based on MPLS VC label.

- `mpls-tunnel-label`
  - Link selection policy is based on MPLS tunnel label.

- `mpls-vc-tunnel-label`
  - Link selection policy is based on the combination of MPLS VC and tunnel label.
Example:

The following example creates and add port 16,17,18 and 19 to virtual trunk.

```
switch(config)# virtual-trunk
Creating New virtual Trunk :: 1

switch(config-virtual-trunk-1)# ports extreme-ethernet 0/16-19
```

This virtual trunk can be assigned to an output of configuration map. For example 10G traffic coming from the network on input ports 3 and 4 can be load balanced to virtual trunk 1.

```
switch(config)# configuration map
Creating New Configuration Map :: 1

switch(config-map-1)# input-ports extreme-ethernet 0/3,0/4 output-ports vtrunk 1
```

### 6.5 Filter Templates

Filter templates are used to specify filtering for specific traffic criteria. After a filter template has been created, it can then be applied to a configuration map. There are 3 unique types of templates: MAC based, IP based, or UDB (user-defined bytes) based.

**CLI Command:**

```
filter-mac access-list template <access-list-number (1-65535)>
filter-ip access-list template <access-list-number (1001-65535)>
filter-udb access-list template <access-list-number (1-50)>
```

**Syntax Description:**

Enters into filter templates edit mode. It is mandatory to specify an access list number within the template type’s range. The “no” version of this command deletes the specified filter template.

**CLI Command:**

```
permit { any | host <src-mac-address>} { any | host <dest-mac-address>} [{aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000|etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-id | <protocol (0-65535)>}|{encaptype <value (1-65535)>}|{Vlan <vlan-id (1-4094)>}|{priority <value (1-255)>}]
```
**aarp**

EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address

**dec-spanning**

EtherType Digital Equipment Corporation (DEC) spanning tree

**decnet-iv**

EtherType DECnet Phase IV protocol

**diagnostic**

EtherType DEC-Diagnostic

**dsm**

EtherType DEC-DSM/DDP

**etype-6000**

EtherType 0x6000

**etype-8042**

EtherType 0x8042

**lat**

EtherType DEC-LAT

**lavc-sca**

EtherType DEC-LAVC-SCA

**mop-console**

EtherType DEC-MOP Remote Console

**mop-dump**

EtherType DEC-MOP Dump

**msdos**

EtherType DEC-MSDOS

**mumps**

EtherType DEC-MUMPS

**netbios**

EtherType DEC- Network Basic Input/Output System (NETBIOS)

**vines-echo**

EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems

**vines-ip**

EtherType VINES IP

**xns-id**

EtherType Xerox Network Systems (XNS) protocol suite

**encaptype**

Encapsulation Type

deny { any | host <src-mac-address> } { any | host <dest-mac-address> } [aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-id | <protocol (0-65535)> | [vlan <vlan-id (1-4094)> | [priority <value (1-255)> | [encaptype <value (1-65535)>]]

**Syntax Description**

any | host <src-mac-address> - Source MAC address to be matched with the packet

any | host <dest-mac-address> - Destination MAC address to be matched with the packet
<table>
<thead>
<tr>
<th>Ethertype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aarp</td>
<td>AppleTalk Address Resolution Protocol that maps a data-link address to a network address</td>
</tr>
<tr>
<td>amber</td>
<td>EtherType DEC-Amber</td>
</tr>
<tr>
<td>dec-spanning</td>
<td>EtherType Digital Equipment Corporation (DEC) spanning tree</td>
</tr>
<tr>
<td>decnet-iv</td>
<td>EtherType DECnet Phase IV protocol</td>
</tr>
<tr>
<td>diagnostic</td>
<td>EtherType DEC-Diagnostic</td>
</tr>
<tr>
<td>dsm</td>
<td>EtherType DEC-DSM/DDP</td>
</tr>
<tr>
<td>etype-6000</td>
<td>EtherType 0x6000</td>
</tr>
<tr>
<td>etype-8042</td>
<td>EtherType 0x8042</td>
</tr>
<tr>
<td>lat</td>
<td>EtherType DEC-LAT</td>
</tr>
<tr>
<td>lavc-sca</td>
<td>EtherType DEC-LAVC-SCA</td>
</tr>
<tr>
<td>mop-console</td>
<td>EtherType DEC-MOP Remote Console</td>
</tr>
<tr>
<td>mop-dump</td>
<td>EtherType DEC-MOP Dump</td>
</tr>
<tr>
<td>msdos</td>
<td>EtherType DEC-MSDOS</td>
</tr>
<tr>
<td>mumps</td>
<td>EtherType DEC-MUMPS</td>
</tr>
<tr>
<td>netbios</td>
<td>EtherType DEC- Network Basic Input/Output System (NETBIOS)</td>
</tr>
<tr>
<td>vines-echo</td>
<td>Virtual Integrated Network Service (VINES) Echo from Banyan Systems</td>
</tr>
<tr>
<td>vines-ip</td>
<td>EtherType VINES IP</td>
</tr>
<tr>
<td>xns-id</td>
<td>EtherType Xerox Network Systems (XNS) protocol suite</td>
</tr>
<tr>
<td>encaptype</td>
<td>Encapsulation Type</td>
</tr>
</tbody>
</table>

**CLI Command:**

`set name <mac-filter-name>`

**Syntax Description:**

Specifies name for the MAC filter template.
CLI Command:

```
set description <mac-filter-desc>
```

Syntax Description:
Specifies description for the MAC filter template.

CLI Command:

```
No filter-mac access-list template <access-list-number (1-65535)>
```

Syntax Description:
Deletes filter template from the system.

CLI Command:

```
filter-ip access-list template <access-list-number (1001-65535)>
```

Syntax Description:
This command allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched.

CLI Command:

```
permit { ip | ospf | pim | <protocol-type (1-255)>}{ any | host <src-ip-address> | <src-ip-address> <mask> }{ any | host <dest-ip-address> | <dest-ip-address> <mask> }[ {tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>} ] [priority <value (1-255)>]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip | ospf | pim | <protocol-type (1-255)> | Source IP address can be
| any | host | <src-ip-address> | * 'any' or
| <src-ip-address> | the dotted decimal address or
| <mask> | * the IP Address of the network or the host that the packet is from and the network mask to use with the source address. |
| any | host | <dest-ip-address> | Destination IP address can be
| <dest-ip-address> | * 'any' or
| <mask> | * the dotted decimal address or
| | * the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address |
tos - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.

priority - The priority of the L3 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of 'filter priority' implies a higher priority.

CLI Command:

deny { ip | ospf | pim | <protocol-type (1-255)>}{ any | host <src-ip-address> | <src-ip-address> <mask> }{ any | host <dest-ip-address> | <dest-ip-address> <mask> }{ tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>}[priority <value (1-255)>]

Syntax Description:

deny { ip | ospf | pim | <protocol-type (1-255)>}{ any | host <src-ip-address> | <src-ip-address> <mask> }{ any | host <dest-ip-address> | <dest-ip-address> <mask> }{ tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>}[priority <value (1-255)>]

CLI Command:

permit ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr><integer(0-128)> } { any | host <ip6_addr> <integer(0-128)> } }
<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow-label</td>
<td>Flow identifier in IPv6 header.</td>
</tr>
<tr>
<td>any</td>
<td>host &lt;ip6_addr&gt; &lt;integer(0-128)&gt;</td>
</tr>
<tr>
<td>any</td>
<td>host &lt;ip6_addr&gt; &lt;integer(0-128)&gt;</td>
</tr>
</tbody>
</table>

**CLI Command:**

deny ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr> <integer(0-128)> } } { any | host <ip6_addr> <integer(0-128)> } }

**Syntax Description:**
This command specifies the TCP packets to be forwarded based on the associated parameters.

**CLI Command:**

permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> }[{gt <port-number (1-65535)> | lt <port-number (1-65535)>|eq <port-number (1-65535)> |range <port-number (1-65535)> <port-number (1-65535)>}]{ any | host <dest-ip-address> | <dest-ip-address> <dest-mask> }[{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range <port-number (1-65535)> <port-number (1-65535)>}][{ack | rst }][{tos{max-reliability|max-throughput|min-delay|normal}<tos-value(0-7)>}][dscp <value (0-63)>][ priority <short(1-255)>]

**Syntax Description:**
- **any** | **host**
  - **<src-ip-address>**
  - **<src-ip-address> <src-mask>**
  - Source IP address can be
    - 'any' or the dotted decimal address OR
    - the IP address of the network or the host that the packet is from and the network mask to use with the source address

- **port-number**
  - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.
    - eq=equal
    - lt=less than
    - gt=greater than
    - range=a range of ports; two different port numbers must be specified
any|host
<dest-ip-address>
|<dest-ip-address>
< dest-mask > - Destination IP address can be
  - ‘any’ or
  - the dotted decimal address or
  - the IP Address of the network or the host that
    the packet is destined for and the network mask
    to use with the destination address

ack - TCP ACK bit to be checked against the packet. It can be
  establish (1), non-establish (2) or any (3).

rst - TCP RST bit to be checked against the packet. It can be
  set (1), not set (2) or any (3).

tos - Type of service. Can be max-reliability, max throughput,
  min-delay, normal or a range of values from 0 to 7,
  Differentiated Services Code Point (DSCP) values to
  match against incoming packets.

priority - The priority of the filter is used to decide which filter rule
  is applicable when the packet matches with more than
  one filter rules. Lower value of ‘filter priority’ implies a
  higher priority.

CLI Command:

deny tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> }
{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}
{ any | host <dest-ip-address> | <dest-ip-address> <dest-mask> }
{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}
{ack | rst }
{tos{max-reliability|max-throughput|min-delay|normal}<tos-value(0-7)>
|dscp <value (0-63)>}
[ priority <short(1-255)>]

Syntax
Description

any|host - Source IP address can be
  - ‘any’ or
  - the dotted decimal address OR
  - the IP address of the network or the host that
    the packet is from and the network mask to use
    with the source address

<src-ip-address> - Port Number. The input for the source and the
  destination port-number is prefixed with one of the
  following operators.
  - eq=equal
  - lt=less than
  - gt=greater than
  - range=a range of ports; two different port
    numbers must be specified
any|host
<dest-ip-address> - Destination IP address can be
|<dest-ip-address>
< dest-mask >  - 'any' or
- the dotted decimal address or
- the IP Address of the network or the host that
  the packet is destined for and the network mask
to use with the destination address

ack - TCP ACK bit to be checked against the packet. It can be
establish (1), non-establish (2) or any (3).

rst - TCP RST bit to be checked against the packet. It can be
set (1), not set (2) or any (3).

tos - Type of service. Can be max-reliability, max throughput,
min-delay, normal or a range of values from 0 to 7,
Differentiated Services Code Point (DSCP) values
to match against incoming packets.
priority - The priority of the filter is used to decide which filter rule
is applicable when the packet matches with more than
one filter rules. Lower value of 'filter priority' implies a
higher priority.

Syntax Description:

This command specifies the UDP packets to be forwarded based on the associated parameters.

CLI Command:

permit udp { any | host <src-ip-address> | <src-ip-address> <src-mask>}{(gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535) > <port-number (1-65535)>}){ any | host <dest-ip-address> | <dest-ip-address> <dest-mask> }{[ (gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>)]{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}} [ priority <(1-255)>]

Syntax Description

udp - User Datagram Protocol

any| host
<src-ip-address>| - Source IP address can be
<src-ip-address>
<src-mask>  - 'any' or
- the word 'host' and the dotted decimal address
or
- number of the network or the host that the
  packet is from and the network mask to use with
  the source address
### Port-Number

- Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.
  - `eq` = equal
  - `lt` = less than
  - `gt` = greater than
  - `range` = a range of ports; two different port numbers must be specified

### Any|Host

- Destination IP address can be
  - ‘any’ or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is destined for and the network mask to use with the destination address

### Tos

- Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.

### Priority

- The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of ‘filter priority’ implies a higher priority.

### CLI Command:

```plaintext
deny udp { any | host src-ip-address | src-ip-address src-mask } { gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)> } { any | host dest-ip-address | dest-ip-address dest-mask } { gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)> } { tos { max-reliability | max-throughput | min-delay | normal | <tos-value (0-7)> } | dscp <value (0-63)> } [ priority <(1-255)> ]
```

Syntax Description:

- **Udp**
  - User Datagram Protocol

- **Any|Host**
  - Source IP address can be
    - ‘any’ or
    - the word 'host' and the dotted decimal address or
    - number of the network or the host that the packet is from and the network mask to use with the source address
port-number  - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.
  - eq=equal
  - lt=less than
  - gt=greater than
  - range=a range of ports; two different port numbers must be specified

any|host
<dest-ip-address>
<dest-ip-address>
<dest-mask>  - Destination IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is destined for and the network mask to use with the destination address

tos
{max-reliability
 | max-throughput
 | min-delay
}
| normal | <value (0-7)> | dscp
<value(0-63)>  - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.
priority  - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of 'filter priority' implies a higher priority.

Syntax Description:

This command specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.

CLI Command:

```
permit icmp {any | host <src-ip-address>|<src-ip-address> <mask>} {any | host <dest-ip-address> | <dest-ip-address> <mask>} [<message-type (0-255)>] [<message-code (0-255)>] [ priority <(1-255)>]
```

Syntax Description:

```
icmp
any| host
<src-ip-address>
<src-ip-address>
<mask>  - Source IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is from and the network mask to use with the source address
```
any|host
<dest-ip-address>|<dest-ip-address>
<mask>

- Destination IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is destined for and the network mask to use with the destination address

message-type

- Message type

message-code

- ICMP Message code

priority

- The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of 'filter priority' implies a higher priority.

CLI Command:

```
deny icmp {any | host <src-ip-address>|<src-ip-address> <mask>}{any | host <dest-ip-address>|<dest-ip-address> <mask>}{message-type (0-255)}{message-code (0-255)} [ priority {(1-255)}]
```

Syntax Description

- icmp - Internet Control Message Protocol

any| host
<src-ip-address>|<src-ip-address>
<mask>

- Source IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is from and the network mask to use with the source address

any|host
<dest-ip-address>|<dest-ip-address>
<mask>

- Destination IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is destined for and the network mask to use with the destination address

message-type

- Message type

message-code

- ICMP Message code

priority

- The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of 'filter priority' implies a higher priority.
CLI Command:
   `set name <ip-filter-name>`

Syntax Description:
Specifies name for the IP filter template.

CLI Command:
   `set description <ip-filter-desc>`

Syntax Description:
Specifies description for the IP filter template.

CLI Command:
   `no filter-ip access-list template <access-list-number> (1001-65535)`

Syntax Description:
Deletes filter template from the system.

CLI Command:
   `filter-udb access-list template <access-list-number> (1-50)`

Syntax Description:
This command permits packets matching a particular User Defined Byte and by specifying the packet type – namely user-defined, tcp-ipv4, udp, mpls, ipv4, ipv6, frag-ip.

CLI Command:
   `permit user-defined-packet-type { user-def | tcp-ipv4 | udp-ipv4 | mpls | ipv4 | ipv6 | frag-ip } offset-base {12 | 13 | 14 | ipv6-ext hdr | ether-type | <short(0-127)>} offset1 <short(0-127)> <short(0-255)> [offset2 <short(0-127)> <short(0-255)> [offset3 <short(0-127)> <short(0-255)> [offset4 <short(0-127)> <short(0-255)> [offset5 <short(0-127)> <short(0-255)> [offset6 <short(0-127)> <short(0-255)>] priority <short (1-255)>]

Syntax Description
- `user-def` - Specifies the packet type as user defined.
- `tcp-ipv4` - Specifies the packet type as tcp in the ipV4 packet.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>udp-ipv4</strong></td>
<td>Specifies the packet type as udp in the ipv4 packet.</td>
</tr>
<tr>
<td><strong>mpls</strong></td>
<td>Specifies the packet type as mpls.</td>
</tr>
<tr>
<td><strong>ipv4</strong></td>
<td>Specifies the packet type as ipv4.</td>
</tr>
<tr>
<td><strong>ipv6</strong></td>
<td>Specifies the packet type as ipv6.</td>
</tr>
<tr>
<td><strong>frag-ip</strong></td>
<td>Specifies the packet type as fragmented ip.</td>
</tr>
<tr>
<td><strong>offset-base</strong></td>
<td>Specifies the start of the packet from which the user defined byte should be considered.</td>
</tr>
<tr>
<td></td>
<td>l2 – Start of the packet is considered as layer 2</td>
</tr>
<tr>
<td></td>
<td>l3 – Start of the packet is considered as layer 3</td>
</tr>
<tr>
<td></td>
<td>l4 – Start of the packet is considered as layer 4</td>
</tr>
<tr>
<td></td>
<td>ipv6-ext hdr - Start of the packet is considered as ipv6 extended header.</td>
</tr>
<tr>
<td></td>
<td>ether-type – Start of the packet is considered as ether type.</td>
</tr>
<tr>
<td><strong>offset1</strong></td>
<td>Specifies the offset position and offset value that needs to be considered as the match for offset 1. The two input value ranges 0 to 127 and 0 to 255.</td>
</tr>
<tr>
<td><strong>offset2</strong></td>
<td>Specifies the offset position and offset value that needs to be considered as the match for offset 2. The two input value ranges 0 to 127 and 0 to 255.</td>
</tr>
<tr>
<td><strong>offset3</strong></td>
<td>Specifies the offset position and offset value that needs to be considered as the match for offset 3. The two input value ranges 0 to 127 and 0 to 255.</td>
</tr>
<tr>
<td><strong>offset4</strong></td>
<td>Specifies the offset position and offset value that needs to be considered as the match for offset 4. The two input value ranges 0 to 127 and 0 to 255.</td>
</tr>
<tr>
<td><strong>offset5</strong></td>
<td>Specifies the offset position and offset value that needs to be considered as the match for offset 5. The two input value ranges 0 to 127 and 0 to 255.</td>
</tr>
<tr>
<td><strong>offset6</strong></td>
<td>Specifies the offset position and offset value that needs to be considered as the match for offset 6. The two input value ranges 0 to 127 and 0 to 255.</td>
</tr>
</tbody>
</table>

**CLI Command:**

```bash
deny  usr-defined-packet-type { user-def | tcp-ipv4 | udp-ipv4 | mpls | ipv4 | ipv6 | frag-ip } offset-base {l2 | l3 | l4 | ipv6-ext-hdr | ether-type | <short(0-127)> } offset1 <short(0-127)> <short(0-255)>[offset2 <short(0-127)> <short(0-255)>][offset3 <short(0-127)> <short(0-255)>][offset4 <short(0-127)> <short(0-255)>][offset5 <short(0-127)> <short(0-255)>][offset6 <short(0-127)> <short(0-255)>] priority <short (1-255)>
```
<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-def</td>
<td>- Specifies the packet type as user defined.</td>
</tr>
<tr>
<td>tcp-ipv4</td>
<td>- Specifies the packet type as tcp in the ipV4 packet.</td>
</tr>
<tr>
<td>udp-ipv4</td>
<td>- Specifies the packet type as udp in the ipV4 packet.</td>
</tr>
<tr>
<td>mpls</td>
<td>- Specifies the packet type as mpls.</td>
</tr>
<tr>
<td>ipv4</td>
<td>- Specifies the packet type as ipv4.</td>
</tr>
<tr>
<td>ipv6</td>
<td>- Specifies the packet type as ipv6.</td>
</tr>
<tr>
<td>frag-ip</td>
<td>- Specifies the packet type as fragmented ip.</td>
</tr>
<tr>
<td>offset-base</td>
<td>- Specifies the start of the packet from which the user defined byte should be considered.</td>
</tr>
<tr>
<td></td>
<td>l2 – Start of the packet is considered as layer 2</td>
</tr>
<tr>
<td></td>
<td>l3 – Start of the packet is considered as layer 3</td>
</tr>
<tr>
<td></td>
<td>l4 – Start of the packet is considered as layer 4</td>
</tr>
<tr>
<td></td>
<td>ipv6-ext-hdr - Start of the packet is considered as ipv6 extended header.</td>
</tr>
<tr>
<td></td>
<td>ether-type – Start of the packet is considered as ether type.</td>
</tr>
<tr>
<td>offset1</td>
<td>- Specifies the offset position and offset value that needs to be considered as the match for offset1. The two input value ranges 0 to 127 and 0 to 255.</td>
</tr>
<tr>
<td>offset2</td>
<td>- Specifies the offset position and offset value that needs to be considered as the match for offset 2. The two input value ranges 0 to 127 and 0 to 255.</td>
</tr>
<tr>
<td>Offset3</td>
<td>- Specifies the offset position and offset value that needs to be considered as the match for offset 3. The two input value ranges 0 to 127 and 0 to 255.</td>
</tr>
<tr>
<td>Offset4</td>
<td>- Specifies the offset position and offset value that needs to be considered as the match for offset 4. The two input value ranges 0 to 127 and 0 to 255.</td>
</tr>
<tr>
<td>Offset5</td>
<td>- Specifies the offset position and offset value that needs to be considered as the match for offset 5. The two input value ranges 0 to 127 and 0 to 255.</td>
</tr>
<tr>
<td>Offset6</td>
<td>- Specifies the offset position and value that needs to be considered as the match for offset 6. The two input value ranges 0 to 127 and 0 to 255.</td>
</tr>
</tbody>
</table>
CLI Command:

   set name <udb-filter-name>

Syntax Description:
Specifies name for the UDB filter template.

CLI Command:

   set description <udb-filter-desc>

Syntax Description:
Specifies description for the UDB filter template.

CLI Command:

   no filter-udb access-list template <access-list-number (1-50)>

Syntax Description:
Deletes filter template from the system.

Example:
The following example creates a filter template that is set to only pass TCP traffic.

```
Switch(config)# IM(config)# filter-ip access-list template 1002
Creating New Ip Filter Template :: 1002

Switch(config-filter-ip-1002)# permit tcp any any priority 1
```

This filter template can be assigned to a configuration map. For example, network traffic coming in on ports 1 and 2 can be forwarded to a monitoring appliance on port 3

```
Switch(config)# configuration map
Creating New Configuration Map :: 1

Switch(config-map-1)# input-ports extreme-ethernet 0/1,0/2 output-ports 0/3

Switch(config-map-1)# filter template ip 1002
```
6.6 swap-priority cfg-map1 cfg-map2

Swaps the priority of the first configuration map argument with the priority of the second configuration map argument. The integer specifies the configuration map’s IDs.

\[\text{swap-priority \texttt{cfg-map1 <integer(1-4000)> \texttt{cfg-map2 <integer(1-4000)>}} \]

**Syntax**
- `cfg-map1` - specifies the configuration map ID of the first configuration map
- `cfg-map2` - specifies the configuration map ID of the second configuration map

**Description**
- `integer(1-4000)` - polling interval

**Mode**
- Global Configuration Mode

**Example**
Switch(config)# swap-priority cfg-map1 1 cfg-map2 2

6.7 set filter-match poll-time-interval

Specifies the polling interval for filter counters.

\[\text{set filter-match \texttt{poll-time-interval \texttt{<integer(1-1000)>}}} \]

**Syntax**
- `integer(1-1000)` - polling interval

**Mode**
- Global Configuration Mode

**Example**
Switch(config)# set filter-match poll-time-interval 500

6.8 set tagging-mode

When VLAN stripping is used, specifies whether one or two VLAN tags will be stripped on the egress.

\[\text{set tagging-mode \{ \texttt{single | double} \}} \]

**Syntax**
- `single` - only one VLAN tag will be stripped
- `double` - two VLAN tags will be stripped

**Mode**
- Global Configuration Mode

**Example**
Switch(config)# set tagging-mode double
6.9 set hash-mode

Specifies the hash algorithm used for port channel based load balancing. Packet-xor mode uses an XOR based algorithm to perform load balancing. The two CRC based modes use a CRC polynomial equation to perform load balancing.

```plaintext
set hash-mode { packet-xor | crc6 [<integer(0-63)>] | crc16 [<integer(0-65535)>] }
```

- **Syntax**
- **Description**
  - packet-xor - sets hash mode to packet-XOR
  - crc6 - sets hash mode to CRC6
  - crc16 - sets hash mode to CRC16

- **Mode**
  - Global Configuration Mode

- **Example**
  - `Switch(config)# set hash-mode crc6`

6.10 set l2-vpn-mpls-strip

Enables or disables layer 2 MPLS stripping for a specific interface.

```plaintext
set l2-vpn-mpls-strip { enable | disable }
```

- **Syntax**
- **Description**
  - enable - enables L2 MPLS stripping
  - disable - disables L2 MPLS stripping

- **Mode**
  - Interface Configuration Mode

- **Example**
  - `Switch(config-if)# set l2-vpn-mpls-strip disable`

6.11 set name

Specifies a name for the given port.

```plaintext
set name <port-name>
```

- **Syntax**
- **Description**
  - port-name - Name for the given port.

- **Mode**
  - Interface Configuration Mode

- **Example**
  - `Switch(config-if)# set name "P1"`
6.12 set description

Specifies a description for the given port.

```plaintext
set description <port-desc>
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-desc</td>
<td>Description for the given port.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-if)# set description &quot;Garland 4224 input&quot;</td>
</tr>
</tbody>
</table>

6.13 set nested-vlan

Allows packet to be forwarded based on port VLAN configuration.

```plaintext
set nested-vlan { enable | disable }
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enables nested VLAN functionality</td>
</tr>
<tr>
<td>disable</td>
<td>disables nested VLAN functionality</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-if)# set nested-vlan disable</td>
</tr>
</tbody>
</table>

6.14 set in-traffic

Allows or blocks incoming traffic for a specific interface.

```plaintext
set in-traffic { allow | block }
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>allows incoming traffic</td>
</tr>
<tr>
<td>block</td>
<td>blocks incoming traffic</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-if)# set in-traffic block</td>
</tr>
</tbody>
</table>

6.15 set out-traffic

Allows or blocks outgoing traffic for a specific interface.

```plaintext
set out-traffic { allow | block }
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>allows outgoing traffic</td>
</tr>
<tr>
<td>block</td>
<td>blocks outgoing traffic</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Configuration Mode</td>
</tr>
</tbody>
</table>
6.16 **set crc-hash**

Specifies the hash policy for CRC based hashing on a per-port basis.

```
set crc-hash ([src-mac][dest-mac][mpls-vc-label][mpls-tunnel-label][mpls-vc-tunnel-label][src-ip-byte0][src-ip-byte1] [src-ip-byte2] [src-ip-byte3] [dest-ip-byte0] [dest-ip-byte1] [dest-ip-byte2] [dest-ip-byte3][src-ip6][dest-ip6][ipv6-flow][src-port][dest-14-port][src-14-port])
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>src-mac</td>
<td>source MAC address based hash</td>
</tr>
<tr>
<td>dest-mac</td>
<td>destination MAC based hash</td>
</tr>
<tr>
<td>mpls-vc-label</td>
<td>MPLS VC label based hash</td>
</tr>
<tr>
<td>mpls-tunnel-label</td>
<td>MPLS tunnel label based hash</td>
</tr>
<tr>
<td>mpls-vc-tunnel-label</td>
<td>MPLS tunnel and VC label based hash</td>
</tr>
<tr>
<td>src-ip-byte0</td>
<td>first byte of source IP based hash</td>
</tr>
<tr>
<td>src-ip-byte1</td>
<td>second byte of source IP based hash</td>
</tr>
<tr>
<td>src-ip-byte2</td>
<td>third byte of source IP based hash</td>
</tr>
<tr>
<td>src-ip-byte3</td>
<td>fourth byte of source IP based hash</td>
</tr>
<tr>
<td>dest-ip-byte0</td>
<td>first byte of destination IP based hash</td>
</tr>
<tr>
<td>dest-ip-byte1</td>
<td>second byte of destination IP based hash</td>
</tr>
<tr>
<td>dest-ip-byte2</td>
<td>third byte of destination IP based hash</td>
</tr>
<tr>
<td>dest-ip-byte3</td>
<td>fourth byte of destination IP based hash</td>
</tr>
<tr>
<td>src-ip6</td>
<td>source IPv6 address based hash</td>
</tr>
<tr>
<td>dest-ip6</td>
<td>destination IPv6 address based hash</td>
</tr>
<tr>
<td>ipv6-flow</td>
<td>IPv6 flow label based hash</td>
</tr>
<tr>
<td>src-port</td>
<td>source port based hash</td>
</tr>
<tr>
<td>dest-14-port</td>
<td>layer 4 destination port based hash</td>
</tr>
<tr>
<td>src-14-port</td>
<td>layer 4 source port based hash</td>
</tr>
</tbody>
</table>

**Mode** Interface Configuration Mode

**Example**

```
Switch(config-if)# set crc-hash-policy src-ip-byte0 src-14-port
```
6.17 set link-mode

Sets a link to a regular status, a status of forced up, or a status of listen mode for a specific interface. Force link up mode is normally used when a device (such as a passive TAP) without a TX laser is connected to the FAB. This mode forces the link up so that egress traffic will continue to flow from the specific port.

`set link-mode { regular | forced | listen }`

**Syntax**
- regular - the port is in a normal state
- forced - the port is forced up
- listen - the port is in listen mode

**Mode**
Interface Configuration Mode

**Example**
```
Switch(config-if)# set link-mode forced
```

6.18 show port mpls-strip-details

Shows whether MPLS stripping for L2 VPN traffic is enabled or not per port.

`show port mpls-strip-details`

**Syntax**
- n/a

**Mode**
Privileged/User EXEC Mode

**Example**
```
Switch# show port mpls-strip-details
 Interface L2-vpn-mpls-strip
--------- -----------------
 Ex0/1    Disabled
 Ex0/2    Disabled
 Ex0/3    Disabled
 Ex0/4    Disabled
 Ex0/5    Disabled
 Ex0/6    Disabled
 Ex0/7    Disabled
 Ex0/8    Disabled
```

6.19 show port name

Displays the name of the specific interfaces.

`show port name`

**Syntax**
- n/a

**Description**
- n/a
6.20  show port description

Displays the description of the specific interfaces.

show port description

Syntax  n/a

Description  

Mode  Privileged/User EXEC Mode

Example  Switch# show port description

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ex0/1</td>
<td>Physical Port</td>
</tr>
<tr>
<td>Ex0/2</td>
<td>Physical Port</td>
</tr>
<tr>
<td>Ex0/3</td>
<td>Physical Port</td>
</tr>
<tr>
<td>Ex0/4</td>
<td>Physical Port</td>
</tr>
<tr>
<td>Ex0/5</td>
<td>Physical Port</td>
</tr>
<tr>
<td>Ex0/6</td>
<td>Physical Port</td>
</tr>
<tr>
<td>Ex0/7</td>
<td>Physical Port</td>
</tr>
<tr>
<td>Ex0/8</td>
<td>Physical Port</td>
</tr>
</tbody>
</table>

6.21  show tagging-mode

Displays whether VLAN stripping will remove one or two VLAN tags from the packet.

show tagging-mode

Syntax  n/a

Description  

Mode  Privileged/User EXEC Mode

Example  Switch# show tagging-mode

Tagging Mode : Single
6.22 show nested-vlan info

Displays the current status per port of nested VLAN.

Syntax
show nested-vlan info

Description
n/a

Mode
Privileged/User EXEC Mode

6.23 show in-traffic info

Displays a list of all of the interfaces and shows whether incoming traffic is allowed or blocked per port.

Syntax
show in-traffic info

Description
n/a

Mode
Privileged/User EXEC Mode

Example
Switch# show in-traffic info

<table>
<thead>
<tr>
<th>Interface</th>
<th>In-Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ex0/1</td>
<td>allow</td>
</tr>
<tr>
<td>Ex0/2</td>
<td>allow</td>
</tr>
<tr>
<td>Ex0/3</td>
<td>allow</td>
</tr>
<tr>
<td>Ex0/4</td>
<td>allow</td>
</tr>
<tr>
<td>Ex0/5</td>
<td>allow</td>
</tr>
<tr>
<td>Ex0/6</td>
<td>allow</td>
</tr>
<tr>
<td>Ex0/7</td>
<td>allow</td>
</tr>
<tr>
<td>Ex0/8</td>
<td>allow</td>
</tr>
</tbody>
</table>

6.24 show out-traffic info

Displays a list of all of the interfaces and shows whether outgoing traffic is allowed or blocked per port.

Syntax
show out-traffic info

Description
n/a

Mode
Privileged/User EXEC Mode

Example
Switch# show out-traffic info

<table>
<thead>
<tr>
<th>Interface</th>
<th>Out-Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ex0/1</td>
<td>allow</td>
</tr>
</tbody>
</table>
### 6.25 show global hash-mode

Displays the current global hash mode information for load balancing.

```
show global hash-mode
Syntax: n/a
Description: n/a
Mode: Privileged/User EXEC Mode
Example:
Switch# show global hash-mode
Hash-mode: packet-xor
```

### 6.26 show crc-hash-policy

Displays the current CRC hash policy information used for load balancing.

```
show crc-hash-policy
Syntax: n/a
Description: n/a
Mode: Privileged/User EXEC Mode
Example:
Switch# show crc-hash-policy
Policy Index : 0
----------------
Source Mac Address
Destination Mac Address
Mpls-vc-label
Mpls-tunnel-label
Mpls-vc-tunnel-label
Source IP Address Byte0
Source IP Address Byte1
Source IP Address Byte2
Source IP Address Byte3
Destination IP Address Byte0
Destination IP Address Byte1
Destination IP Address Byte2
Destination IP Address Byte3
Destination IPv6 Address
Source IPv6 Address
IPv6 Flow
```
6.27 show hash-mode-info

Displays whether CRC hashing mode is enabled per port and displays the CRC hashing policy used per port.

show hash-mode-info

Syntax: n/a

Mode: Privileged/User EXEC Mode

Example:

Switch# show hash-mode-info

<table>
<thead>
<tr>
<th>Interface</th>
<th>Crc-HashMode</th>
<th>Policy-Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ex0/1</td>
<td>Enabled</td>
<td>0</td>
</tr>
<tr>
<td>Ex0/2</td>
<td>Enabled</td>
<td>0</td>
</tr>
<tr>
<td>Ex0/3</td>
<td>Enabled</td>
<td>0</td>
</tr>
<tr>
<td>Ex0/4</td>
<td>Enabled</td>
<td>0</td>
</tr>
<tr>
<td>Ex0/5</td>
<td>Enabled</td>
<td>0</td>
</tr>
<tr>
<td>Ex0/6</td>
<td>Enabled</td>
<td>0</td>
</tr>
<tr>
<td>Ex0/7</td>
<td>Enabled</td>
<td>0</td>
</tr>
<tr>
<td>Ex0/8</td>
<td>Enabled</td>
<td>0</td>
</tr>
</tbody>
</table>

6.28 show link-mode info

Displays the port setting for each port. The setting can be regular, forced, or listen.

show link-mode info

Syntax: n/a

Mode: Privileged/User EXEC Mode

Example:

Switch# show force-link-up info

<table>
<thead>
<tr>
<th>Interface</th>
<th>Link Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ex0/1</td>
<td>Disabled</td>
</tr>
<tr>
<td>Ex0/2</td>
<td>Disabled</td>
</tr>
<tr>
<td>Ex0/3</td>
<td>Disabled</td>
</tr>
<tr>
<td>Ex0/4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Ex0/5</td>
<td>Disabled</td>
</tr>
<tr>
<td>Ex0/6</td>
<td>Disabled</td>
</tr>
<tr>
<td>Ex0/7</td>
<td>Disabled</td>
</tr>
<tr>
<td>Ex0/8</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
6.29 **show filter-match poll-time-interval**

Displays the polling interval for filter match counts.

```
show filter-match poll-time-interval
```

**Syntax**

n/a

**Description**

Mode

- Privileged/User EXEC Mode

**Example**

```
Switch# show filter-match poll-time-interval
Filter-Matches Poll-Time-Interval : 1 Second
```

6.30 **show filter-match count**

Displays the number of packets matching specific filters.

```
show filter-match count
```

**Syntax**

n/a

**Description**

Mode

- Privileged/User EXEC Mode

**Example**

```
Switch# show filter-match count

<table>
<thead>
<tr>
<th>Filter</th>
<th>Filter-Type</th>
<th>Match-Pkt-Count</th>
<th>Match-Byte-Count</th>
<th>Bits/Sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>IP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

6.31 **clear filter-match**

Clears the specified filter counters.

```
clear filter-match \{ all | \{filter-id <integer(1-65535)> type \{mac \{ip \{udb\}\}\} \} \} | type \{mac \{ip \{udb\}\}\} \}
```

**Syntax**

- **all** - Clears all filter counters
- **filter-id** - Specifies a specific filter to clear
- **type** - Specifies the type of filter that was specified by filter-id, or if filter-id is not specified, will clear all filters of the specified type

**Mode**

- Privileged/User EXEC Mode

**Example**

```
Switch# clear filter-match type ip
```
### 6.32 show port-group

Displays all port channel and virtual trunk port groups configured.

**Syntax**

```
show port-group
```

**Description**

n/a

**Mode**

Privileged/User EXEC Mode

**Example**

```
Switch# show port-group

Id : 18
Type : Port Channel
Name : PO18
Desc : Enter description here
Ports : Ex0/1, Ex0/2
```

### 6.33 show configuration map

Displays specific or all configuration maps that have been configured.

**Syntax**

```
show configuration map { <integer(1-4000)> | all }
```

**Description**

- `integer(1-4000)` - Displays specific configuration map
- `all` - Displays all configuration maps

**Mode**

Privileged/User EXEC Mode

**Example**

```
Switch# show configuration map all

-----------------------------------------------
Config Map : 1
Input Ports : Ex0/3, Ex0/4
Output Ports : Ex0/7
IP Filter's : 1002
Filter Priority : 2997
Description : Security Websense Monitoring
Name : Websense Monitor
Status : Enabled
Advance Action : None
Filter Mode : Pass All
Commit Mode : Enabled
Privilege :
```
6.34 **show access-lists**

This command displays the access lists configuration.

```
show access-lists [[{ip | mac | user-defined }] < access-list-number (1-65535)> ]
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>- IP Access List</td>
</tr>
<tr>
<td>mac</td>
<td>- MAC Access List</td>
</tr>
<tr>
<td>user-defined</td>
<td>- user defined access list</td>
</tr>
</tbody>
</table>

**Mode**

Privileged/User EXEC Mode

**Example**

```
Switch# show access-lists
EIP ACCESS LISTS
-----------------
```

**Standard IP Access List 34**

```
------------------
IP address Type   : IPV4
Source IP address : 172.30.3.134
Source IP address mask : 255.255.255.255
Source IP Prefix Length : 32
Destination IP address : 0.0.0.0
Destination IP address mask : 0.0.0.0
Destination IP Prefix Length : 0
Flow Identifier : 0
In Port List : NIL
Out Port List : NIL
Filter Action : Deny
Status : InActive
```

**Extended IP Access List 1002**

```
------------------
Filter Priority : 1
Filter Protocol Type : ANY
IP address Type : IPV4
Source IP address : 0.0.0.0
Source IP address mask : 0.0.0.0
Source IP Prefix Length : 0
Destination IP address : 0.0.0.0
Destination IP address mask : 0.0.0.0
Destination IP Prefix Length : 0
Flow Identifier : 0
In Port List : NIL
Out Port List : NIL
Filter TOS : Invalid combination
Filter DSCP : NIL
Filter Action : Permit
Status : InActive
```

**MAC ACCESS LISTS**

```
------------------
No MAC Access Lists have been configured
```
Chapter 7

7. FAB Port Security

The FAB system is capable of high level security that can grant or restrict users privileges to sections of the configuration including system settings and configuration maps. This high level of security can grant or deny users privileges to the individuals ports as well.

The following are the list of FAB security related commands:

- add user
- set user
- no user
- show user
- add group
- set group description
- set group default-privilege
- no group
- show group
- add member user
- no group member
- show port privilege

7.1 Security Configuration Overview

Security is provided to areas of the configuration or individual ports by granting access to groups that are created. Individual user privileges are provided by group membership.

The levels of security that are granted are “none”, “access”, “modify”, or “full”. Granting a group “full” privileges to any are configuration section or port is equivalent to granting that group “root” access. This allows any member of that group to grant privileges to other groups.
7.2 add user

Command Description – adds a user to the FAB and assigns a password.

add user <username> password <password>

Syntax

username - logon name to assign to the user
password - password to assign to the user

Mode

Global Configuration Mode

Example

Switch(config)# add user ezekial password p$y0p0c3rhe
% add user ezekial successfully with user id 6

Related Commands

- show user - Displays the information about users configured in the FAB.

7.3 set user

Command Description – changes the password for a user that has been previously configured.

set user <userid> password <password>

Syntax

userid - user number that was assigned to a user name
password - password to assign to the user

Mode

Global Configuration Mode

Example

Switch(config)# set user 6 password %0hc@ralt
% set user 6 successfully

Related Commands

- show user - Displays the information about users configured in the FAB.

7.4 no user

Command Description – deletes a user from the FAB.

no user <userid>

Syntax

userid - user number that was assigned to a user name

Mode

Global Configuration Mode

Example

Switch(config)# no user 4
delete user 4 successfully
7.5 **show user**

Command Description – displays users that have been configured in the FAB

```
show user {<userid> | active | all}
```

**Syntax**
- `userid` - the ID number for a user
- `active` - Users currently logged into the FAB
- `all` - displays information about all configured users

**Mode** Privileged/User EXEC Mode

**Example**
```
Switch(config)# show user all
UserId  Username
------  --------
 1      root
 2      dale
 3      joe
```

7.6 **add group**

Command Description – adds a group that users will become members of. Groups will be assigned security privileges to the FAB configuration sections and ports.

```
add user <groupname> [description <description>]
```

**Syntax**
- `groupname` - name that will identify a security group
- `description` - optional description to help document group properties

**Mode** Global Configuration Mode

**Example**
```
Switch(config)# add group ModifySystemSettings description "Can Modify System Settings But Not Maps"
% add group ModifySystemSettings successfully with group id 6
```

**Related Commands**
- `show group` - Displays the information about groups configured in the FAB.
8. FAB Port Speed

The FAB system can be set to fixed speeds as well as auto negotiation. Additionally, the FAB has the ability to display information about any SFP that is plugged into a port.

The following are the list of FAB speed and SFP related commands:

- set force-speed
- show port force-speed
- show port sfp

8.1 Port Speed Configuration Overview

Occasionally, devices connected to each other do not properly negotiate the speed that they should communicate at, when auto negotiation is used.

By forcing a speed on both sides of a link, a user can guarantee that devices will properly communicate at the right speed, thus eliminating issues when two devices do not appear to be talking to one another.

8.2 set force-speed

Command Description – forces the speed on a port to a fixed speed or auto negotiation.

```
set force-speed { 1G | 10G | 40G | auto }
```

**Syntax**

```
force-speed
```

- can be set to 1G, 10G, 40G, or auto

**Mode**

Global Configuration Mode

**Example**

```
Switch(config-if)# set force-speed 10G
```

**Related Commands**

- `show force-speed` – displays the speeds of the ports on the FAB.
8.3 show port force-speed

Command Description – displays the speed on all ports in the FAB.

set port force-speed

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>force-speed</td>
<td>will display 1G, 10G, 40G, or auto</td>
</tr>
</tbody>
</table>

Mode

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

Switch# show port force-speed

<table>
<thead>
<tr>
<th>Interface</th>
<th>Force-Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ex0/1</td>
<td>10G</td>
</tr>
<tr>
<td>Ex0/2</td>
<td>auto</td>
</tr>
<tr>
<td>Ex0/3</td>
<td>auto</td>
</tr>
<tr>
<td>Ex0/4</td>
<td>auto</td>
</tr>
<tr>
<td>Ex0/5</td>
<td>auto</td>
</tr>
<tr>
<td>Ex0/6</td>
<td>auto</td>
</tr>
<tr>
<td>Ex0/7</td>
<td>auto</td>
</tr>
<tr>
<td>Ex0/8</td>
<td>auto</td>
</tr>
</tbody>
</table>

Related Commands

- set force-speed – forces speeds of ports on the FAB.

8.4 show port sfp

Command Description – displays information on all SFP transceivers in the FAB.

show port sfp

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port sfp</td>
<td>displays information on each SFP.</td>
</tr>
</tbody>
</table>

Mode

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

Switch# show port sfp

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vendor</th>
<th>VPN</th>
<th>Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ex0/1</td>
<td>FINISAR CORP.</td>
<td>FTLX8571D3BCL</td>
<td>10G</td>
</tr>
<tr>
<td>Ex0/2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ex0/3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ex0/4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ex0/5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ex0/6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ex0/7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ex0/8</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>