GARLAND

TECHNOLOGY

FAB10Gxxxx
FAB40Gxxxx

FAB CLI Command Line
Reference Manual

Firmware Revision Level: 42XX_8.10-xx

Garland Technology
Buffalo, New York and Garland, Texas
Office: 716-242-8500
support@garlandtechnology.com
www.garlandtechnology.com

DISCLAIMER The information in this book is provided “as is”, with no warranties whatsoever, including any warranty of merchantability, fitness for any particular purpose or any warranty otherwise arising out of any proposal, specification or sample. This document is provided for informational purposes only and should not be construed as a commitment on the part of Garland Technology. Information in this document is subject to change without notice.

REQUESTS For information or obtaining permission for use of material of this work, please submit a written request to: Corporate Marketing and Legal, Garland Technology on www.garlandtechnology.com

DOCUMENT No.: Garland Technology FAB-CLI_v8.x-GT-rev3

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

6.23 SHOW IN-TRAFFIC INFO....47
6.24 SHOW OUT-TRAFFIC INFO....47
6.25 SHOW GLOBAL HASH-MODE....48
6.26 SHOW CRC-HASH-POLICY....48
6.27 SHOW HASH-MODE-INFO....49
6.28 SHOW LINK-MODE INFO....49
6.29 SHOW FILTER-MATCH POLL-TIME-INTERVAL....50
6.30 SHOW FILTER-MATCH COUNT....50
6.31 CLEAR FILTER-MATCH....50
6.32 SHOW PORT-GROUP....51
6.33 SHOW CONFIGURATION MAP....51
6.34 SHOW ACCESS-LISTS....52
CHAPTER 7: FAB PORT SECURITY 53
7.1 SECURITY CONFIGURATION OVERVIEW....53
7.2 ADD USER....54
7.3 SET USER....54
7.4 NO USER....54
7.5 SHOW USER....55
7.6 ADD GROUP....55
CHAPTER 8: FAB PORT SPEED 56
8.1 PORT SPEED CONFIGURATION OVERVIEW....56
8.2 SET FORCE-SPEED....56
8.3 SHOW PORT FORCE-SPEED....57
8.4 SHOW PORT SFP....57

Chapter
1

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

Up Arrow / Down Arrow	Displays the previously executed command
Ctrl + C	Exits from the SWITCH prompt
Backspace / Ctrl + H	Removes a single character
TAB	Completes a command without typing the full word
Left Arrow / Right Arrow	Traverses the current line

Others

- ? - helps to list the available 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

Command Mode	Access Method	Prompt	Exit method
User EXEC	This is the initial mode to start a session.	**`Switch>`**	The logout method is used.
Privileged EXEC	The User EXEC mode command **`enable`**, is used to enter the Privileged EXEC mode.	**`Switch#`**	To return from the Privileged EXEC mode to User EXEC mode the **`disable`** command is used.
Global Configuration	The Privileged EXEC mode command **`configure terminal`**, is used to enter the Global Configuration mode.	**`Switch(config)#`**	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.
Interface Configuration	The Global Configuration mode command **`interface <interface-type><interface-id>`** is used to enter the Interface configuration mode.	**`Switch(config-if)#`**	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.
Config-VLAN	The global configuration mode command **`vlan vlan-id`**, is used to enter the Config-VLAN mode.	**`Switch(config-vlan)#`**	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.
Line Configuration	The global configuration mode command **`line`**, is used to enter the Line Configuration mode.	**`Switch(config-line)#`**	To exit to the Global Configuration mode the **`exit`** command is used and to exit to the Privileged EXEC mode the **`end`** command is used.

2.2 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.

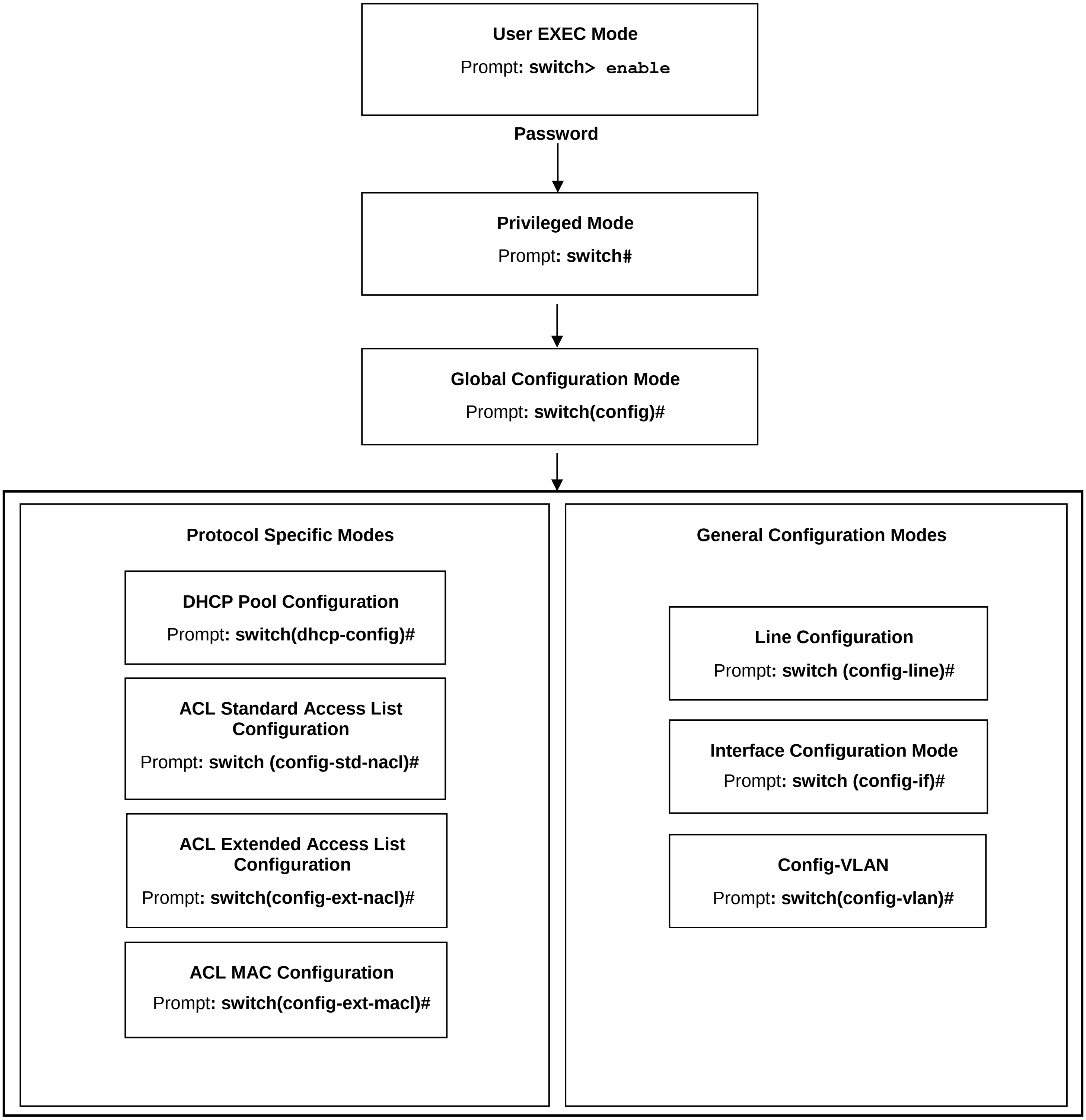
User EXEC Mode
Prompt: switch> enable
Password
Privileged Mode
Prompt: switch#
Global Configuration Mode
Prompt: switch(config)#
Protocol Specific Modes
DHCP Pool Configuration
Prompt: switch(dhcp-config)#
ACL Standard Access List Configuration
Prompt: switch (config-std-nacl)#
ACL Extended Access List 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

Chapter 3

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}]
```

Syntax Description	`channel-group-number`	-	Number of the channel group. Valid numbers range from maximum number of ports in the system to maximum number of aggregations supported
	`detail`	-	Detailed EtherChannel information
	`load-balance`	-	Load-balance or frame-distribution scheme among ports in the port channel
	`port`	-	EtherChannel port information

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

                LACP Port  Admin Oper   Port    Port
Port     State   Priority  Key   Key    Number  State
-----------------------------------------------------
Ex0/1    Bundle  128        1      1      0x1     0xbe

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 Description **etherchannel** - Interface EtherChannel information

Mode Privileged EXEC Mode

Example

```
Switch# show interfaces ex 0/1 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,


                 LACP Port   Admin  Oper   Port    Port
Port     State   Priority    Key    Key    Number  State
-------------------------------------------------------------
Ex0/1    Bundle  128         2      2      0x1     0x3c

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 Wait-time  = 2 secs
LACP Activity : Passive
LACP Timeout : Long

Aggregation State : Aggregation, Sync, Collecting, Distributing,

Port : Ex0/2
-------------

Port State = Up in Bundle
Channel Group : 2
Mode : Active
```

```
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,

                 LACP Port   Admin  Oper   Port    Port
Port     State   Priority    Key    Key    Number  State
-------------------------------------------------------------
Ex0/1    Bundle  128         2      2      0x1     0x3c
Ex0/2    Bundle  128         2      2      0x2     0x3c

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

Chapter

4

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-sha1]) }
```

```
no ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth ([hmac-md5] [hmac-sha1]) }
```

Syntax Description	**version compatibility**	-	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 Description

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

enable – enables Telnet access

disable – disables Telnet access

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}
```

Syntax Description

`integer` - Specifies the port mirroring configuration to be set.

`source` - Sets the specified interface as the source port(s) to be mirrored

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

`tx` - Only traffic sent out on the specified port will be mirrored to the destination port.

`rx` - Only traffic received on the specified port will be mirrored to the destination port.

`both` - All traffic transmitted and received on the specified port will be mirrored to the destination port.

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 Description	**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, ouput 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     - Specifiy 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)>] l3-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.
l3-vpn-mpls-strip – Strip MPLS label from l3-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:

This command specifies the packets to be forwarded based on the MAC address and the associated parameters, that is, this command allows non-IP traffic to be forwarded if the conditions are matched.

```
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)>][encaptype <value (1-65535)>][Vlan <vlan-id (1-4094)>][priority <value (1-255)>]

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

aarp	Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address
amber	EtherType DEC-Amber
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

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-addresq> | <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	**ip| ospf|pim| <protocol-type (1-255)>**	-	Type of protocol for the packet. It can also be a protocol number.
	any| host <src-ip-address>| <src-ip-address> <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.
	any|host <dest-ip-address>| <dest-ip-address> <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

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-addresq> | <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

ip| ospf|pim| <protocol-type (1-255)> - Type of protocol for the packet. It can also be a protocol number.

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

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

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.

Syntax Description:

This command specifies IP packets to be forwarded based on protocol and associated parameters.

CLI Command:

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

Syntax Description	flow-label	-	Flow identifier in IPv6 header.
	any | host <ip6_addr> <integer(0-128)>	-	Source address of the host / any host.
	any | host <ip6_addr> <integer(0-128)>	-	Destination address of the host / any host.

CLI Command:

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

Syntax	flow-label	-	Flow identifier in IPv6 header.
Description	any | host <ip6_addr> <integer(0-128)>	-	Source address of the host / any host.
	any | host <ip6_addr> <integer(0-128)>	-	Destination address of the host / any host.

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	tcp	-	Transport Control Protocol
	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), notset (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

tcp - Transport Control Protocol

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), notset (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>| <src-ip-address> <src-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

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.

CLI Command:

```
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 <src-ip-address>| <src-ip-address> <src-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

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 - 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:

```
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  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)>
```

Syntax Description	**user-def**	-	Specifies the packet type as user defined.
	tcp-ipv4	-	Specifies the packet type as tcp in the ipV4 packet.

udp-ipv4 - Specifies the packet type as udp in the ipV4 packet.

mpls - Specifies the packet type as mpls.

ipv4 - Specifies the packet type as ipv4.

ipv6 - Specifies the packet type as ipv6.

frag-ip - Specifies the packet type as fragmented ip.

offset-base - Specifies the start of the packet from which the user defined byte should be considered.
l2 – Start of the packet is considered as layer 2
l3 – Start of the packet is considered as layer 3
l4 – Start of the packet is considered as layer 4
ipv6-ext-hdr - Start of the packet is considered as ipv6 extended header.
ether-type – Start of the packet is considered as ether type.

offset1 - 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.

offset2 - Specifies the offset position and offset value value that needs to be considered as the match for offset 2. The two input value ranges 0 to 127 and 0 to 255.

Offset3 - 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.

Offset4 - 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.

Offset5 - 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.

Offset6 - 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.

CLI Command:

```
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)>
```

Syntax Description

`user-def` - Specifies the packet type as user defined.

`tcp-ipv4` - Specifies the packet type as tcp in the ipV4 packet.

`udp-ipv4` - Specifies the packet type as udp in the ipV4 packet.

`mpls` - Specifies the packet type as mpls.

`ipv4` - Specifies the packet type as ipv4.

`ipv6` - Specifies the packet type as ipv6.

`frag-ip` - Specifies the packet type as fragmented ip.

`offset-base` - Specifies the start of the packet from which the user defined byte should be considered.
l2 – Start of the packet is considered as layer 2
l3 – Start of the packet is considered as layer 3
l4 – Start of the packet is considered as layer 4
ipv6-ext-hdr - Start of the packet is considered as ipv6 extended header.
ether-type – Start of the packet is considered as ether type.

`offset1` - 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.

`offset2` - Specifies the offset position and offset value value that needs to be considered as the match for offset 2. The two input value ranges 0 to 127 and 0 to 255.

`Offset3` - 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.

`Offset4` - 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.

`Offset5` - 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.

`Offset6` - 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.

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.

```
swap-priority cfg-map1 <integer(1-4000)> cfg-map2 <integer(1-4000)>
```

Syntax Description	**cfg-map1 – specifies the configuration map ID of the first configuration map** **cfg-map2 – specifies the configuration map ID of the second configuration map**
Mode	Global Configuration Mode
Example	`Switch(config)# swap-priority cfg-map1 1 cfg-map2 2`
Mode	Global Configuration Mode
Example	`Switch(config)# set parse-ip-header disable`

6.7 set filter-match poll-time-interval

Specifies the polling interval for filter counters.

```
set filter-match poll-time-interval <integer(1-1000)>
```

Syntax Description	**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.

```
set tagging-mode { single | double }
```

Syntax Description	**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.

```
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.

```
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.

```
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.

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

Syntax Description	`port-desc – Description for the given port.`
Mode	Interface Configuration Mode
Example	`Switch(config-if)# set description "Garland 4224 input"`

6.13 set nested-vlan

Allows packet to be forwarded based on port VLAN configuration.

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

Syntax Description	`enable – enables nested VLAN functionality`
	`disable – disables nested VLAN functionality`

Mode	Interface Configuration Mode
Example	`Switch(config-if)# set nested-vlan disable`

6.14 set in-traffic

Allows or blocks incoming traffic for a specific interface.

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

Syntax Description	`allow – allows incoming traffic`
	`block -  blocks incoming traffic`

Mode	Interface Configuration Mode
Example	`Switch(config-if)# set in-traffic block`

6.15 set out-traffic

Allows or blocks outgoing traffic for a specific interface.

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

Syntax Description	`allow – allows outgoing traffic`
	`block -  blocks outgoing traffic`

Mode Interface Configuration Mode

Example

```
Switch(config-if)# set out-traffic block
```

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-l4-port][src-l4-port])
```

Syntax Description	`src-mac`	- source MAC address based hash
	`dest-mac`	- destination MAC based hash
	`mpls-vc-label`	- MPLS VC label based hash
	`mpls-tunnel-label`	- MPLS tunnel label based hash
	`mpls-vc-tunnel-label`	- MPLS tunnel and VC label based hash
	`src-ip-byte0`	- first byte of source IP based hash
	`src-ip-byte1`	- second byte of source IP based hash
	`src-ip-byte2`	- third byte of source IP based hash
	`src-ip-byte3`	- fourth byte of source IP based hash
	`dest-ip-byte0`	- first byte of destination IP based hash
	`dest-ip-byte1`	- second byte of destination IP based hash
	`dest-ip-byte2`	- third byte of destination IP based hash
	`dest-ip-byte3`	- fourth byte of destination IP based hash
	`src-ip6`	- source IPv6 address based hash
	`dest-ip6`	- destination IPv6 address based hash
	`ipv6-flow`	- IPv6 flow label based hash
	`src-port`	- source port based hash
	`dest-l4-port`	- layer 4 destination port based hash
	`src-l4-port`	- layer 4 source port based hash

Mode Interface Configuration Mode

Example

```
Switch(config-if)# set crc-hash-policy src-ip-byte0 src-l4-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 Description

```
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 Description 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 Description n/a

Mode Privileged/User EXEC Mode

Example

```
Switch# show port name
 Interface    Name
---------    ----
Ex0/1        P1
Ex0/2        P2
Ex0/3        P3
Ex0/4        P4
Ex0/5        P5
Ex0/6        P6
Ex0/7        P7
Ex0/8        P8
```

6.20 show port description

Displays the description of the specific interfaces.

show port description

Syntax Description **n/a**

Mode Privileged/User EXEC Mode

Example

```
Switch# show port description
 Interface    Description
---------    -----------
Ex0/1        Physical Port
Ex0/2        Physical Port
Ex0/3        Physical Port
Ex0/4        Physical Port
Ex0/5        Physical Port
Ex0/6        Physical Port
Ex0/7        Physical Port
Ex0/8        Physical Port
```

6.21 show tagging-mode

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

show tagging-mode

Syntax Description **n/a**

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.

show nested-vlan info

Syntax 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.

show in-traffic info

Syntax Description n/a

Mode Privileged/User EXEC Mode

Example

```
Switch# show in-traffic info

 Interface     In-Traffic
---------     -----------
Ex0/1         allow
Ex0/2         allow
Ex0/3         allow
Ex0/4         allow
Ex0/5         allow
Ex0/6         allow
Ex0/7         allow
Ex0/8         allow
```

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.

show out-traffic info

Syntax Description n/a

Mode Privileged/User EXEC Mode

Example

```
Switch# show out-traffic info

Interface     Out-Traffic
---------     -----------
Ex0/1         allow
```

```
Ex0/2         allow
Ex0/3         allow
Ex0/4         allow
Ex0/5         allow
Ex0/6         allow
Ex0/7         allow
Ex0/8         allow
```

6.25 show global hash-mode

Displays the current global hash mode information for load balancing.

show global hash-mode

Syntax 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 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
```

```
Source Port
Destination L4 Port
Source L4 Port
```

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 Description n/a

Mode Privileged/User EXEC Mode

Example

```
Switch# show hash-mode-info

Interface     Crc-HashMode        Policy-Index
---------     ----------------    ----------
Ex0/1         Enabled             0
Ex0/2         Enabled             0
Ex0/3         Enabled             0
Ex0/4         Enabled             0
Ex0/5         Enabled             0
Ex0/6         Enabled             0
Ex0/7         Enabled             0
Ex0/8         Enabled             0
```

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 Description n/a

Mode Privileged/User EXEC Mode

Example

```
Switch# show force-link-up info

Interface     Link Mode
---------     ----------------
Ex0/1         Disabled
Ex0/2         Disabled
Ex0/3         Disabled
Ex0/4         Disabled
Ex0/5         Disabled
Ex0/6         Disabled
Ex0/7         Disabled
Ex0/8         Disabled
```

6.29 show filter-match poll-time-interval

Displays the polling interval for filter match counts.

show filter-match poll-time-interval

Syntax Description n/a

Mode Privileged/User EXEC Mode

Example

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

6.30 show filter-match count

Displays the number of packets matching specific filters.

show filter-match count

Syntax Description n/a

Mode Privileged/User EXEC Mode

Example

```
Switch# show filter-match count

Filter   Filter-Type  Match-Pkt-Count     Match-Byte-Count   Bits/Sec
------   -----------  -----------------   -----------------  --------
 1001        IP               0                  0               0
```

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 Description

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.

show port-group

Syntax 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.

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

Syntax 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)>]

Syntax Description

ip - IP Access List

mac - MAC Access List

user-defined - user defined access list

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 Description	**username** **password**	- -	logon name to assign to the user 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 Description	**userid** **password**	- -	user number that was assigned to a user name password to assign to the user
Mode	Global Configuration Mode		
Example			

```
Switch(config)# set user 6 password %0hc@ra1t
% 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 Description	**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 Description	**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>]`

`no user <userid>`

Syntax Description	**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.

Chapter

8

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 Description	**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`

Syntax Description **`force-speed`** - **`will display 1G, 10G, 40G, or auto`**

Mode Privileged/User EXEC Mode

Example

```
Switch# show port force-speed
Interface    Force-Speed
---------    ----
Ex0/1        10G
Ex0/2        auto
Ex0/3        auto
Ex0/4        auto
Ex0/5        auto
Ex0/6        auto
Ex0/7        auto
Ex0/8        auto
```

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`

Syntax Description **`port sfp`** - **`displays information on each SFP.`**

Mode Privileged/User EXEC Mode

Example

```
Switch# show port sfp
Interface    Vendor           VPN              Capabilities
---------    ------           ---              ------------
Ex0/1        FINISAR CORP.    FTLX8571D3BCL    10G
Ex0/2
Ex0/3
Ex0/4
Ex0/5
Ex0/6
Ex0/7
Ex0/8
```

DISCLAIMER The information in this book is provided “as is”, with no warranties whatsoever, including any warranty of merchantability, fitness for any particular purpose or any warranty otherwise arising out of any proposal, specification or sample. This document is provided for informational purposes only and should not be construed as a commitment on the part of Garland Technology. Information in this document is subject to change without notice.

REQUESTS For information or obtaining permission for use of material of this work, please submit a written request to: Corporate Marketing and Legal, Garland Technology on www.garlandtechnology.com

DOCUMENT No.: Garland Technology FAB-CLI_v8.x-GT-rev3

Garland Technology: FAB Switch

Revision Number: 2.0

Garland Technology
Buffalo, New York and Garland, Texas
Office: 716-242-8500
support@garlandtechnology.com
www.garlandtechnology.com