FAB10Gxxxx
FAB40Gxxxx

FAB CLI User Manual

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

DOCUMENT No.: Garland Technology FAB-CLI_v2.0-GT-rev2

Contents

.

Chapter 1

1.Introduction

1.1 Purpose

Garland Technology FAB is a pre-integrated OEM ready software for managed Layer2/Layer 3 switches, which performs switching between Ethernet ports at wire speed. **Garland Technology FAB** provides the basic bridging functionality and also offers advanced features such as link aggregation, GVRP/GMRP, IGMP Snooping and Network Access Control.

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

1.2 Scope

The scope of this document is limited to **Garland Technology FAB** release 5.0.0.0. This document details all the Marvell xCAT based CLI 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.
- Garland Technology SWITCH is available in three different packages, namely, Workgroup, Enterprise and Metro1. The parameters specific for a particular package are indicated along with the description of the parameter itself.

1.4 Key Conventions

1.4.1 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

1.4.2 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

[1] Refer SWITCH Product Specification Document for a detailed description of the package.

Chapter 2

2.Command Line Interface

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

The Command Line Interface (CLI) can be used to configure the Intelligent Switch Solution from a console attached to the serial port of the switch or from a remote terminal using TELNET.

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 **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.

When **Garland Technology FAB-Chassis** 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: chassisuser

Password: ********

Switch#-boot>

The Boot Configuration mode is now available to the user.

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.

Command Mode	Access Method	Prompt	Exit method
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.
Redundancy Configuration	The global configuration mode command **redundancy**, is used to enter the Redundancy Configuration mode.	**switch(config-r)#**	To exit to the Global Configuration mode the **exit** command is used.
Bypass segment configuration mode	The global configuration mode command **bypass segment <segment-id>** is used to enter the bypass segment configuration mode for the specified segment-id	**switch(config-bypass-segment)#**	To exit to the Global Configuration mode the **exit** command is used.
Boot Configuration	This is the initial mode to start an SWITCH-Chassis session.	**switch-boot>**	The **reload** command is used to restart the Switch.

2.2 User EXEC Mode

After logging into the device, the user is automatically 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 following are the different modes present under the Interface Configuration mode.

2.5.1 Physical Interface Mode

The Physical Interface mode is used to perform interface specific operations. To return to the global configuration mode the **exit** command is used.

2.5.2 Port Channel Interface Mode

The Port Channel Interface mode is used to perform port-channel specific operations.

To return to the global configuration mode the **exit** command is used.

2.5.3 VLAN Interface Mode

The VLAN Interface mode is used to perform L3-IPVLAN specific operations. To return to the global configuration mode the **exit** command is used.

2.5.4 Tunnel Interface Mode

The Tunnel Interface mode is used to perform Tunnel specific operations. To return to the global configuration mode the **exit** command is used.

2.5.5 Out of Band Interface Mode

The Out of Band Interface mode is used to perform OOB interface specific operations. To return to the global configuration mode 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.

2.8 Boot Configuration

This mode is used to generate the Slot information (module type). The **reload** command is used to restart the Switch.

2.9 Redundancy Configuration

This mode is used to modify the redundancy parameters. To return to the global configuration mode the **exit** command is used.

2.10 Protocol Specific Modes

The following are the different Protocol specific modes.

2.10.1 DiffSrv ClassMap Configuration mode

The class-map global configuration command creates a class map to be used for matching the packets to the class whose index is specified and to enter the class-map configuration mode The Global configuration mode command **`class-map <short(1-65535)>`** is used to enter the DiffSrv ClassMap Configuration mode and. the prompt seen at this mode is switch(**`config-cmap)#`**.

To return to the global configuration mode the **`exit`** command is used.

2.10.2 DiffSrv Policy-Map Configuration Mode

In the Policy-Map Configuration mode the user can create or modify a policy map.

The Global configuration mode command **`policy-map <short(1-65535)>`** is used to enter the DiffSrv PolicyMap Configuration mode and the prompt seen at this mode is switch**`(config-pmap)#`**.

To return to the global configuration mode the **`exit`** command is used.

2.10.3 DiffSrv Policy-Map Class Configuration Mode

The Policy-Map Class Configuration command defines a traffic classification for the policy to act on. The class-map-num that is specified in the policy map ties the characteristics for that class and its match criteria as configured by using the **`class-map`** global configuration command to the class map. Once the **`class`** command is entered, the switch enters policy-map class configuration mode.

The DiffSrv Policy mode command **`policy-map <short(1-65535)>`** is used to enter the DiffSrv Policy-Map Class Configuration mode and. the prompt seen at this mode is switch**`(config-pmap-c)#`**.

To return to the global configuration mode the **`exit`** command is used.

2.10.4 DHCP Pool Configuration Mode

This mode is used to configure the network pool / host configurations of a subnet pool.

The Global configuration mode command **`ip dhcp pool <integer(1-2147483647)>`** creates a DHCP server address pool and places the user in DHCP pool configuration mode. The prompt seen at this mode is switch**`(dhcp-config)#`**.

To return to the global configuration mode the **`exit`** command is used.

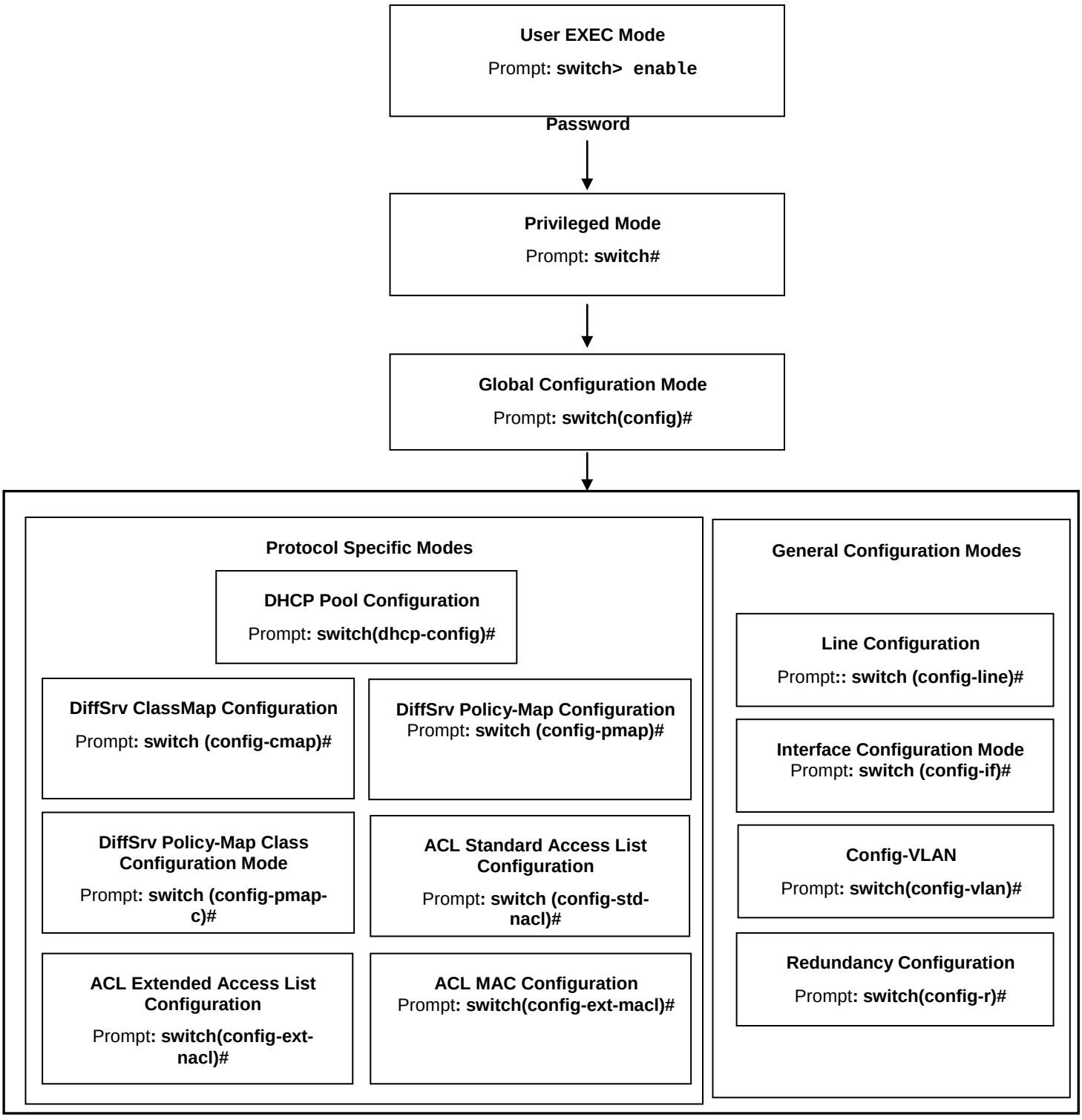

Figure 2-1: Command Modes Access Path

Chapter 3

3.TACACS

TACACS (Terminal Access Controller Access Control System), widely used in network environments, is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for providing NAS (Network Access Security). NAS ensures secure access from remotely connected users. TACACS implements the TACACS Client and provides the AAA (Authentication, Authorization and Accounting) functionalities.

TACACS is used for several reasons:

- Facilitates centralized user administration.
- Uses TCP for transport to ensure reliable delivery.
- Supports inbound authentication, outbound authentication and change password request for the Authentication service.
- Provides some level of protection against an active attacker.

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

- tacacs-server host
- tacacs use-server address
- tacacs-server retransmit
- debug tacacs
- show tacacs

3.1 tacacs-server host

This command configures the TACACS server with the parameters (host, timeout, key). The no form of the command deletes server entry from the TACACS server table.

tacacs-server host {<ipv4-address> | <ipv6-address> | <host-name>} [single-connection] [port <tcp port (1-65535)>] [timeout <time out in seconds(1-255)>] {key <secret key>}

no tacacs-server host { <ipv4-address> | <ipv6-address>}

Syntax Description	**ipv4-address**	-	IPv4 address of the host
	ipv6-address	-	IPv6 address of the host
	host-name	-	Name of the host
	single-connection	-	Establishes Single TCP connection to communicate with TACACS Server
	Port	-	TCP Port number. This value ranges between 1 and 65535.
	Timeout	-	The time period in seconds for which a client will wait for a response from the server before closing the connection. This value ranges between 1 and 255 seconds.
	Key	-	Per-server encryption key. Specifies the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server. The string length is 64.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	port	-	40
	timeout	-	5 seconds

Example

```
switch(config)# tacacs-server host 12.0.0.100
TACACS+ server configured with default secret key !
```

```
switch(config)# tacacs-server host 2005::33
TACACS+ server configured with default secret key !
```

Related Commands

`show tacacs` - Displays the statistical log information and server for TACACS client

3.2 tacacs use-server address

This command selects a server from the list of servers maintained in the TACACS client and makes the TACACS client to use the specified server. The no form of the command disables the configured TACACS active server.

tacacs use-server address { <ipv4-address> | <ipv6-address>}

no tacacs use-server

Syntax Description	**ipv4-address**	-	IPv4 address of the host
	ipv6-address	-	IPv6 address of the host
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config)# tacacs use-server address 10.0.0.100`		

Related Commands

show tacacs - Displays the statistical log information and server for TACACS client

3.3 tacacs-server retransmit

This command specifies the number of times the client searches the active server from the list of servers maintained in the TACACS client, when active server is not configured. The no form of the command sets the default retries.

tacacs-server retransmit <retries>

no tacacs-server retransmit

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# tacacs-server retransmit 3`

3.4 debug tacacs

This command sets the debug trace level for TACACS client module. The no form of the command disables the debug trace level for TACACS client module.

debug tacacs { all | info | errors | dumptx | dumprx }

no debug tacacs

Syntax Description	**All**	-	All TACACS debug messages
	info	-	TACACS Server information messages
	errors	-	Error code debug messages
	dumptx	-	Transmitted packet dump messages
	dumprx	-	Received packet dump messages
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	Debugging is Disabled		
Example	`switch# debug tacacs all`		

3.5 show tacacs

This command displays the statistical log information and server for TACACS+ client.

show tacacs

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
switch# sh tacacs
Server : 1
Server address           : 12.0.0.100
Address Type             : IPV4
       Single Connection : no
       TCP port          : 49
       Timeout           : 5
       Secret Key        : Garland Technology
Server : 2
Server address           : 2005::33
Address Type             : IPV6
       Single Connection : no
       TCP port          : 4949
       Timeout           : 5
       Secret Key        : Garland Technology
Authen. Starts sent    : 0
Authen. Continues sent : 0
Authen. Enables sent   : 0
Authen. Aborts sent    : 0
Authen. Pass rvcd.     : 0
Authen. Fails rcvd.    : 0
Authen. Get User rcvd. : 0
Authen. Get Pass rcvd. : 0
```

```
Authen. Get Data rcvd. : 0
Authen. Errors rcvd.   : 0
Authen. Follows rcvd.  : 0
Authen. Restart rcvd.  : 0
Authen. Sess. timeouts : 0
Author. Requests sent  : 0
Author. Pass Add rcvd. : 0
Author. Pass Repl rcvd : 0
Author. Fails rcvd.    : 0
Author. Errors rcvd.   : 0
Author Follows rcvd.   : 0
Author. Sess. timeouts : 0
Acct. start reqs. sent : 0
Acct. WD reqs. sent    : 0
Acct. Stop reqs. sent  : 0
Acct. Success rcvd.    : 0
Acct. Errors rcvd.     : 0
Acct. Follows rcvd.    : 0
Acct. Sess. timeouts  : 0
Malformed Pkts. rcvd.  : 0
Socket failures        : 0
Connection failures    : 0
```

Related Commands

- **`tacacs-server host -`** Configures the TACACS server with the parameters
- **`tacacs use-server address -`** Selects a server from the list of servers maintained in the TACACS client and makes the TACACS client to use the specified server

Chapter 4

4.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:

- debug etherchannel
- show etherchannel

4.1 debug etherchannel

This command enables trace messages for link aggregation and the no form of the command disables trace messages for link aggregation.

This command operates similar to that of the command **Error! Reference source not found.**.

debug etherchannel {[all] [detail] [error] [event] [idb]}

no debug etherchannel {[all] [detail] [error] [event] [idb]}

Syntax Description	**all**	-	All traces
	detail	-	Detailed debug traces
	error	-	All failure traces
	event	-	Event traces
	idb	-	Interface descriptor block messages
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch# debug etherchannel detail`		

4.2 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

Package Workgroup, Enterprise and Metro

Example

```
switch# show etherchannel
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

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

```
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 : Gi0/1
-------------

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
-----------------------------------------------
Gi0/1    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

switch# show etherchannel 1  port

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

                Ports in the Group
                ------------------

Port : Gi0/1
-------------

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

Aggregation State : Aggregation, Sync, Collecting, Distributing,

Port : Gi0/2
```

```
-------------

Port State = Up in Bundle
Channel Group : 1
Mode : Active
port-channel = Po1
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,

               LACP Port  Admin Oper   Port  Port
Port     State   Priority  Key   Key Number  State
-----------------------------------------------
Gi0/1    Bundle  128         1      1      0x1     0xbc
Gi0/2    Bundle  128         1      1      0x2     0xbc


switch# show etherchannel 1  port-channel

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
```

```
                Channel Group Listing
                ---------------------
Group : 1
----------

               Port-channels in the group:
               ---------------------------

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

switch# show etherchannel summary

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
```

```
Flags:

D - down         P - in port-channel
I - stand-alone  H - Hot-standby (LACP only)
U - in-use

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel    Protocol   Ports
------------------------------------------------------------
1      Po1(U)          LACP       Gi0/1(P),Gi0/2(D)

switch# show etherchannel 1  protocol

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

switch# show etherchannel load-balance

                Channel Group Listing
                ---------------------
Group : 1
----------
Source & Destination MAC Address
```

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

Related Commands

- **Show interfaces – Displays interface specific port-channel information**

4.3 show etherchannel - Redundancy

This command displays Etherchannel information.

show etherchannel [[channel-group-number] { detail | load-balance | port | port-channel | summary | protocol | redundancy}]

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
	redundancy[2]	-	Synced messages
Mode	Privileged EXEC Mode		
Package	Metro		

Example

```
switch# show etherchannel redundancy
Actor Information for Port : Gi0/1
---------------------------------
Channel Group : 1
Pseudo port-channel = Po1
CurrentWhile Split Interval Tmr Count = 1
```

[2] This feature is not supported.

```
Synced Partner Information for Port : Gi0/1
-----------------------------------

Partner System ID               : 00:11:22:33:44:55
Flags                           : A
LACP Partner Port Priority      : 128
LACP Partner Oper Key           : 1

Port State Flags Decode
-----------------------
Activity : Active
LACP Timeout : Long

Aggregation State : Aggregation, Sync, Collecting, Distributing,

Actor Information for Port : Gi0/2
-------------

Channel Group : 1
Pseudo port-channel = Po1
CurrentWhile Split Interval Tmr Count = 1

Synced Partner Information for Port : Gi0/2
-------------
Partner System ID               : 00:11:22:33:44:55
Flags                           : A
LACP Partner Port Priority      : 128
LACP Partner Oper Key           : 1

Port State Flags Decode
-----------------------
Activity : Active
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting, Distributing,
------------------------------------------------------------------
```

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

4.4 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
Package	Workgroup, Enterprise and Metro
Example	`switch# show interfaces gigabitethernet 0/1 etherchannel`

```
Port : Gi0/1
-------------

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
-------------------------------------------------------------
Gi0/1    Bundle 128         2      2      0x1     0x3c
```

```
switch# show interfaces etherchannel

Port : Gi0/1
-------------

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 : Gi0/2
-------------

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
------------------------------------------------------------
Gi0/1    Bundle 128         2      2      0x1     0x3c
Gi0/2    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

4.5 show lacp

This command displays port-channel traffic/neighbor information.

show lacp [<port-channel(1-65535)>] { counters | neighbor [detail] }

Syntax Description	**port-channel**	-	Number of the channel group
	counters	-	Traffic information
	neighbor	-	Neighbor information
	detail	-	Neighbor detail information
Mode	Privileged EXEC Mode		

Example

```
switch# show lacp 1 counters
      LACPDUs    Marker   Marker Response  LACPDUs
Port Sent Recv Sent  Recv  Sent   Recv    Pkts Err
-----------------------------------------
Channel group: 1
------------------
Gi0/1    394   352    0     0      0     0    0   0
Gi0/2    318   297    0     0      0     0    0   0


switch# show lacp neighbor detail

Flags:
A - Device is in Active mode
P - Device is in Passive mode

Channel group 1 neighbors

Port Gi0/1
----------
```

```
Partner System ID                : 00:01:02:03:04:21
Flags                            : P
LACP Partner Port Priority       : 128
LACP Partner Oper Key            : 2
LACP Partner Port State          : 0x3c

Port State Flags Decode
------------------------
Activity : Passive
LACP Timeout : Long

Aggregation State : Aggregation, Sync, Collecting,
Distributing

Port Gi0/2
----------
Partner System ID                : 00:01:02:03:04:21
Flags                            : P
LACP Partner Port Priority       : 128
LACP Partner Oper Key            : 2
LACP Partner Port State          : 0x3c

Port State Flags Decode
------------------------
Activity : Passive
LACP Timeout : Long

Aggregation State : Aggregation, Sync, Collecting,
Distributing
```

☞ Expressions are case sensitive

Chapter 5

5.Syslog

Syslog is a protocol used for capturing log information for devices on a network. The syslog protocol provides a transport to allow a machine to send event notification messages across IP networks to event message collectors, also known as syslog servers. The protocol is simply designed to transport the event messages.

One of the fundamental tenets of the syslog protocol and process is its simplicity. The transmission of syslog messages may be started on a device without a receiver being configured, or even actually physically present. This simplicity has greatly aided the acceptance and deployment of syslog.

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

- logging
- logging synchronous
- mailserver
- sender mail-id
- receiver mail-id
- cmdbuffs
- service timestamps
- clear logs
- syslog mail
- syslog local storage
- syslog filename-one
- syslog filename-two
- syslog filename-three

- syslog relay - port
- syslog profile
- logging-file
- logging server
- mail server
- syslog relay
- syslog relay transport type
- show logging
- show email alerts
- show syslog role
- show syslog mail
- show syslog local storage
- show logging file
- show logging server
- show mail server
- show syslog relay - port
- show syslog profile
- show syslog relay transport type
- show syslog file-name
- show syslog information

5.1 logging

This command enables Syslog server and configures the Syslog Server IP address, the log-level and other Syslog related parameters. The no form of the command disables Syslog server and resets the configured Syslog server IP address, the log-level and other Syslog related parameters.

logging { <ip-address> | buffered [<size (1-200)>] | console | facility {local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7|}| severity [{ <level (0-7)> | alerts | critical | debugging | emergencies | errors | informational | notification | warnings }] | on }

no logging { <ip-address> | buffered | console | facility | severity | on }

Syntax Description

ip-address	-	Host IP address used as a Syslog server.
buffered	-	Limits Syslog messages displayed from an internal buffer. This size ranges between 1 and 200 entries. . The size feature is optional only in the code using the industrial standard command, otherwise this feature is mandatory.
console	-	Limits messages logged to the console.
facility	-	The facility that is indicated in the message. Can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7.
severity	-	Message severity level. Messages with severity level equal to or high than the specified value are printed asynchronously. This can be configured using numerical value or using the available option. The options are: • 0 | emergencies - System is unusable. • 1 | alerts - Immediate action needed. • 2 | critical - Critical conditions. • 3 | errors - Error conditions. • 4 | warnings - Warning conditions. • 5 | notification - Normal but significant conditions. • 6 | informational - Informational messages. • 7 | debugging – Debugging messages.
alerts	-	Immediate action needed
critical	-	Critical conditions
debugging	-	Debugging messages
emergencies	-	System is unusable
errors	-	Error conditions
informational	-	Information messages

	notification	-	Normal but significant messages
	warnings	-	Warning conditions
	on	-	Syslog enabled
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	console	-	enabled
	severity	-	informational, when no option is selected while configuration. debugging, at system start-up.
	buffered	-	50
	facility	-	local0

Example

```
switch(config)# logging 12.0.0.2
```

- The log file is stored in ASCII text format. The Privileged EXEC command is used to display its contents
- The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or Syslog server
- The existing syslog buffers will not be cleared and none of the configured options will be changed, when the Syslog feature is disabled

Related Command

`show logging` - Displays Logging status and configuration information

5.2 logging synchronous

This command enables synchronous logging of messages.

This command operates similar to that of the command logging.

logging synchronous {severity [{<short (0-7)> | alerts | critical | debugging | emergencies | errors | informational | notification | warnings|all}] | limit <number-of-buffers(size(1-200))}

Syntax Description	**severity**	-	Message severity level. Messages with severity level equal to or high than the specified value are printed asynchronously. This can be configured using numerical value or using the available option. The options are: • 0 | emergencies - System is unusable. • 1 | alerts - Immediate action needed. • 2 | critical - Critical conditions. • 3 | errors - Error conditions. • 4 | warnings - Warning conditions. • 5 | notification - Normal but significant conditions. • 6 | informational - Informational messages. • 7 | debugging – Debugging messages. • all - All messages are printed asynchronously regardless of the severity level.
	limit	-	Number of buffers to be queued for the terminal after which new messages are dropped. This value ranges between 1 and 200 entries.
Mode	Line Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	severity	-	informational, when no option is selected while configuration. debugging, at system start-up.
	limit	-	50
Example	`switch(config-line)# logging synchronous severity 4`		

☞
- The log file is stored in ASCII text format. The Privileged EXEC command is used to display its contents.
- The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or Syslog server.

- The existing syslog buffers will not be cleared and none of the configured options will be changed, when the Syslog feature is disabled.

Related Command

`show logging` - Displays Logging status and configuration information

5.3 mailserver

This command sets the mail server IP address to be used for sending email alert messages and the no form of the command re-sets the mail server IP address used for sending email alert messages.

`mailserver <ip-address>`

`no mailserver`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# mailserver 23.78.67.89`

☞ Initially, the mailserver has to be configured, for the **`show email alerts`** command.

Related Commands

- **`logging`** - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- **`show email alerts`** - Displays email alerts related configuration

5.4 sender mail-id

This command sets the sender mail id and the no form of the command deletes the configured sender mail id.

sender mail-id <mail-id (100)>

no sender mail-id

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	syslog@Garland Technology.com
Example	`switch(config)# sender mail-id plabinik@Garland Technology.com`

☞
- Primarily, the mailserver must have been configured for this command
- The sender and receiver email-ids are mandatory for email alert messages to be sent.

Related Commands

- **mailserver** - Sets the mail server IP address to be used for sending email alert messages
- **logging** - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- **show logging** - Displays Logging status and configuration information
- **show email alerts** - Displays email alerts related configuration
- **receiver mail-id** - Sets the receiver mail id

5.5 receiver mail-id

This command sets the receiver mail id and the no form of the command deletes the configured receiver mail id.

receiver mail-id <mail-id (100)>

no receiver mail-id

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	admin@Garland Technology.com
Example	`switch(config)#receiver mail-id plabinik@Garland Technology.com`

☞
- Primarily, the mailserver must have been configured for this command
- The sender and receiver email-ids are mandatory for email alert messages to be sent

Related Commands

- **mailserver** - Sets the mail server IP address to be used for sending email alert messages
- **logging** - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- **show logging** - Displays Logging status and configuration information
- **show email alerts** - Displays email alerts related configuration
- **sender mail-id** - Sets the sender mail id

5.6 cmdbuffs

This command configures the number of syslog buffers for a particular user.

`cmdbuffs <user name> <no.of buffers (1-200)>`

Syntax Description	**`user name`**	-	User Name
	`no.of buffers`	-	Number of log buffers to be allocated in the system
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	50		
Example	`switch(config)#cmdbuffs Garland Technology 50`		

☞ CLI related events like commands given by the user, login/logout etc can be logged on to the Syslog Server.

Related Commands

- **`logging`** - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- **`show logging`** - Displays Logging status and configuration information

5.7 service timestamps

This command enables timestamp option for logged messages and the no form of the command disables timestamp option for logged messages.

`service timestamps`

`no service timestamps`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	Enabled
Example	`switch(config)#service timestamps`

☞
- When enabled, the messages (log and email alert messages) will hold the time stamp information
- When disabled, the time stamp information will not be carried with the messages sent to the log and mail servers

Related Commands

- **`logging`** - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- **`show logging`** - Displays Logging status and configuration information

5.8 clear logs

This command clears the system syslog buffers.

`clear logs`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# clear logs`

Related Commands

- **`cmdbuffs`** - Configures the number of Syslog buffers for a particular user
- **`logging`** - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- **`show logging`** - Displays Logging status and configuration information

5.9 syslog mail

This command enables the mail option in syslog. The no form of command disables the mail option in syslog.

`syslog mail`

`no syslog mail`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# syslog mail`

Related Commands

- **`show syslog mail`** - Displays the mail option in syslog
- **`mail server table`** - Adds an entry to mail-server table

5.10 syslog local storage

This command enables the syslog local storage. The no form of command disables the syslog local storage.

syslog localstorage

no syslog localstorage

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch (config)# syslog localstorage`

Related Commands

- **show syslog local storage** - Displays the syslog local storage.
- **syslog filename-one** - Configures the file name to store the syslog messages.
- **syslog filename-two** - Configures the file name to store the syslog messages.
- **syslog filename-three** - Configures the file name to store the syslog messages
- **logging-file** - Adds an entry in to file table

5.11 syslog filename-one

This command configures the file name to store the syslog messages. The maximum size of the file name is 32.

`syslog filename-one <string(32)>`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch (config)# syslog filename-one iss1`

☞ Syslog local storage must be enabled.

Related Commands

- **`syslog local storage -`** Enables the syslog local storage
- **`show syslog file-name`** - Displays the Syslog local storage file name
- **`logging-file`** - Adds an entry in to file table
- **`show syslog local storage`** - Displays the syslog local storage.

5.12 syslog filename-two

This command configures the file name to store the syslog messages. The maximum size of the file name is 32.

syslog filename-two <string(32)>

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# syslog filename-two iss2`

☞ Syslog local storage must be enabled.

Related Commands

- **syslog local storage -** Enables the syslog local storage
- **show syslog file-name** - Displays the Syslog local storage file name
- **logging-file** - Adds an entry in to file table
- **show syslog local storage** - Displays the syslog local storage.

5.13 syslog filename-three

This command configures the file name to store the syslog messages. The maximum size of the file name is 32.

`syslog filename-three <string(32)>`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# syslog filename-three iss3`

☞ Syslog local storage must be enabled.

Related Commands

- **`syslog local storage -`** Enables the syslog local storage
- **`show syslog file-name`** - Displays the Syslog local storage file name
- **`logging-file`** - Adds an entry in to file table
- **`show syslog local storage`** - Displays the syslog local storage.

5.14 syslog relay - port

This command sets the syslog port through which it receives the syslog messages. The no form of command sets the syslog port to default port 514.

`syslog relay-port <integer(0-65535)>`

`no syslog relay-port`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# syslog relay-port 500`

☞ Syslog relay must be enabled

Related Commands

- **`syslog relay -`** Changes the syslog role from device to relay
- **`syslog relay transport type -`** Sets the Syslog relay transport type either as udp or tcp
- **`show syslog relay - port -`** Displays the Syslog relay port

5.15 syslog profile

This command sets the profile for reliable syslog. The no form of command sets the profile to default (raw) for Reliable Syslog.

`syslog profile {raw | cooked`[3]**`}`**

`no syslog profile`

Syntax Description	**`raw`**	-	Profile with minimum parameters in the BEEP
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config)# syslog profile raw`		

Related Commands

- **`show syslog profile`** - Displays the Syslog profile.

[3] This feature is not supported. It may be implemented in the future.

5.16 logging-file

This command adds an entry in to file table. The no form of command deletes an entry from the file table.

logging-file <short(0-191)> <string(32)>

no logging-file <short(0-191)> <string(32)>

Syntax Description	**short**	-	Priority of syslog messages. 0-lowest priority, 191-highest priority
	string	-	File-name
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch (config)# logging-file 134 iss1`		

☞ Syslog local storage must be enabled

Related Commands

- **show logging file** - Displays the Syslog file table
- **syslog local storage** - Enables the syslog local storage

5.17 logging server

This command adds an entry in to logging-server table. The no form of command deletes an entry from forward table.

logging-server <short(0-191)> {ipv4 <ucast_addr> | ipv6 <ip6_addr>} [port <integer(0-65535)>] [{udp | tcp | beep}]

no logging-server <short(0-191)> {ipv4 <ucast_addr> |ipv6 <ip6_addr>}

Syntax Description	**short**	-	Priority of syslog messages. 0-lowest priority, 191-highest priority
	ipv4,ipv6	-	Version 4 and Version 6 IP address
	port	-	Port number
	udp, tcp,beep		Sets the transport type as either udp, tcp, beep
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch (config)# logging-server 134 ipv4 12.0.0.3`		

Related Commands

- **show logging server** - Displays the Syslog logging server table

5.18 mail server table

This command adds an entry to mail-server table. The no form of command deletes an entry from mail table.

`mail-server <short(0-191)> {ipv4 <ucast_addr> |ipv6 <ip6_addr>} <string(50)>`

`no mail-server <short(0-191)> {ipv4 <ucast_addr> |ipv6 <ip6_addr>}`

Syntax Description	**`short`**	-	Priority of syslog messages. 0-lowest priority, 191-highest priority
	`ipv4, ipv6`	-	Version 4 and Version 6 IP address
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch (config)# mail-server 134 ipv4 12.0.0.100 root@localhost`		

Related Commands

- **`show mail server`** - Displays the Syslog mail server table
- **`syslog mail`** - Enables the mail option in syslog

5.19 syslog relay

This command changes the syslog role from device to relay. The no form of command changes the syslog role from relay to device.

`syslog relay`

`no syslog relay`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# syslog relay`

Related Commands

- **`show syslog role -`** Displays the syslog role.
- **`syslog relay transport type -`** Sets the Syslog relay transport type either as udp or tcp
- **`syslog relay - port -`** Sets the syslog port through which it receives the syslog messages

5.20 syslog relay transport type

This command sets the Syslog relay transport type either as udp or tcp.

`syslog relay transport type {udp | tcp}`

Syntax Description	**`udp`**	-	Sets the relay transport type as udp
	`tcp`	-	Sets the relay transport type as tcp
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config)# syslog relay transport type udp`		

☞ Syslog relay must be enabled

Related Commands

- **`syslog relay -`** Changes the syslog role from device to relay
- **`show syslog role -`** Displays the syslog role.
- **`show syslog relay transport type -`** Displays the Syslog relay transport type
- **`show syslog relay - port -`** Displays the Syslog relay port.

5.21 show logging

This command displays logging status and configuration information.

show logging

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show logging`

```
System Log Information
----------------------
Syslog logging   : enabled(Number of messages 0)
Console logging  : enabled(Number of messages 0)
TimeStamp option : enabled
Severity logging     : Debugging
Log server IP    : 10.0.0.1
Facility         : Default (local0)
Buffered size    : 100

LogBuffer(0 Entries, 0 bytes)
```

Related Commands

- **logging** - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- **service timestamps** - Enables timestamp option for logged messages

5.22 show email alerts

This command displays configurations related to email alerts.

show email alerts

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro

Example	`switch# show email alerts`
	`Sender email-id : syslog@Garland Technology.com`
	`Receiver email-id : admin@Garland Technology.com`
	`Mail server IP : 12.0.0.3`

Related Commands

- **mailserver** - Sets the mail server IP address to be used for sending email alert messages
- **receiver mail-id** - Sets the receiver mail id
- **sender mail-id** - Sets the sender mail id

5.23 show syslog role

This command displays the syslog role.

show syslog role

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show syslog role` `Syslog Role : Relay`

Related Commands

- **syslog relay** - Changes the syslog role from device to relay

5.24 show syslog mail

This command displays the mail option in syslog.

show syslog mail

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show syslog mail` `Syslog Mail Option : Enabled`

Related Commands

- **syslog mail** – Enables the mail option in syslog

5.25 show syslog local storage

This command displays the syslog local storage.

show syslog localstorage

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show syslog localstorage` `Syslog Localstorage : Enabled`

Related Commands

- **syslog local storage** - Enables the syslog local storage

5.26 show logging file

This command displays the Syslog file table.

show logging-file

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	switch# show logging-file Syslog File Table Information ---------- Priority File-Name -------- ---------- 134 iss1 134 iss2 134 iss3

Related Commands

- **syslog filename-one/syslog filename-two/syslog filename-three** - Gets the users desired file name to store syslog message
- **logging-file** - Adds an entry in to file table

5.27 show logging server

This command displays the Syslog logging server table.

show logging-server

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show logging-server`

```
Syslog Forward Table Information
--------------------------------
Priority  Address-Type  IpAddress  Port  Trans-Type
--------  ------------  ---------  ----  ----------

129        ipv4          12.0.0.2   514  udp

134        ipv4          12.0.0.1   514  udp
```

Related Commands

- **logging server** - Adds an entry in to logging-server table

5.28 show mail server

This command displays the Syslog mail server table.

show mail-server

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show mail-server`

```
Syslog Mail Table Information
 ----------------------------

Priority  Address-Type  IpAddress  Receiver Mail-Id
--------  ------------  ---------  ----------------

134       ipv4           12.0.0.100  root@localhost
```

Related Commands

- **mail server** - Adds an entry to mail-server table

5.29 show syslog relay - port

This command displays the Syslog relay port.

show syslog relay-port

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show syslog relay-port` `Syslog Port    : 251`

Related Commands

- **syslog relay - port** - Sets the syslog port through which it receives the syslog messages
- **syslog relay -** Changes the syslog role from device to relay

5.30 show syslog profile

This command displays the Syslog profile.

show syslog profile

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show syslog profile` `Syslog Profile    : raw`

Related Commands

- **syslog profile** - Sets the profile for reliable syslog

5.31 show syslog relay transport type

This command displays the Syslog relay transport type.

show syslog relay transport type

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show syslog relay transport type` `Syslog Relay Transport type udp`

Related Commands

- **syslog relay transport type** - Sets the Syslog relay transport type either as udp or tcp
- **syslog relay - port** - Sets the syslog port through which it receives the syslog messages
- **syslog relay -** Changes the syslog role from device to relay

5.32 show syslog file-name

This command displays the Syslog local storage file name.

show syslog file-name

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro

Example	`switch# show syslog file-name`
	`Syslog File Name`
	`----------------------`
	`Syslog File-One :iss1`
	
	`Syslog File-Two :iss2`
	
	`Syslog File-Three :iss3`

Related Commands

- **syslog local storage** - Enables the syslog local storage
- **show syslog local storage** - Displays the syslog local storage.
- **syslog filename-one** - Configures the file name to store the syslog messages.
- **syslog filename-two** - Configures the file name to store the syslog messages.
- **syslog filename-three** - Configures the file name to store the syslog messages

5.33 show syslog information

This command displays the Syslog information.

show syslog information

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	switch# show syslog information

```
System Log Information
----------------------
Syslog Localstorage    : Enabled

Syslog Mail Option    : Enabled

Syslog Port    : 251

Syslog Role    : Relay
```

Related Commands

- **syslog local storage** - Enables the syslog local storage
- **syslog mail** – Enables the mail option in syslog
- **syslog relay -** Changes the syslog role from device to relay

Chapter 6

6.SSH

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
- debug ssh
- show ip ssh

6.1 ip ssh

This command enables SSH server on the device and also configures the various parameters associated with SSH server. The no form of the command disables SSH server on the device and also re-sets the various parameters associated with 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		
Package	Workgroup, Enterprise and Metro		
Defaults	version compatibility	-	false
	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

6.2 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
Package	Workgroup, Enterprise and Metro
Package	Workgroup, Enterprise and Metro
Defaults	enable
Example	`switch# ssh enable`

Related Command

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

6.3 debug ssh

This command sets the given trace levels for SSH and the no form of the command re-sets the given SSH trace level.

debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer] [server])

no debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer] [server])

Syntax Description	**all**	-	Initialization and Shutdown Messages
	shut	-	Shutdown Messages
	mgmt	-	Management Messages
	data	-	Data Path Messages
	ctrl	-	Control Plane Messages
	dump	-	Packet Dump Messages
	resource	-	Messages related to all resources except Buffers
	buffer	-	Buffer Messages
	server	-	Server Messages
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	Debugging is Disabled		
Example	`switch# debug ssh all`		

☞ Setting all the bits will enable all the trace levels and resetting them will disable all the trace levels.

Related Command

show ip ssh - Displays SSH server information

6.4 show ip ssh

This command displays SSH server information.

show ip ssh

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro

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

Related Command

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

Chapter 7

7.VLAN

VLANs (Virtual LANs) can be viewed as a group of devices on different physical LAN segments which can communicate with each other as if they were all on the same physical LAN segment, that is, a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible.

VLAN provides the following benefits for switched LANs:

- Improved administration efficiency
- Optimized Broadcast/Multicast Activity
- Enhanced network security
- The list of CLI commands for the configuration of VLAN are common to both **Single Instance and Multiple Instance** except for a difference in the prompt that appears for the Switch with Multiple Instance support.

The prompt for the **Global Configuration Mode** is,

```
switch(config)# set vlan enable
```

The prompt for the **VLAN Configuration Mode** is,

```
switch(config-vlan)# ports gigabitethernet 0/1 untagged gigabitethernet 0/1
forbidden gigabitethernet 0/2 name vl1
```

The **parameters** specific to Multiple Instance are stated so, against the respective parameter descriptions in this document.

The output of the **Show commands** differ for Single Instance and Multiple Instance. Hence both the output are documented while depicting the show command examples.

The list of commands for the configuration of VLAN is as follows::

- set vlan
- vlan
- clear vlan statistics
- ports
- vlan active
- switchport pvid/switchport access vlan
- switchport acceptable-frame-type
- switchport ingress-filter
- port mac-vlan
- port subnet – vlan
- port protocol-vlan
- switchport map protocols-group
- switchport priority default
- switchport mode
- switchport mode dot1q-tunnel
- vlan max-traffic-class
- debug vlan
- show vlan
- show vlan device info
- show vlan device capabilities
- show fid - detail
- show forward-all
- show forward-unregistered
- show vlan traffic-classes
- show vlan port config
- show vlan protocols-group
- show protocol-vlan
- show mac-vlan
- show subnet vlan mapping
- show vlan statistics
- show mac-address-table
- show mac-address-table count
- show mac-address-table static unicast
- show mac-address-table static multicast
- show mac-address-table dynamic unicast

- show mac-address-table dynamic multicast
- show mac-address-table aging-time

The following commands can be executed only in a Linux environment and cannot be executed on the target.

- set vlan
- show vlan counters

7.1 set vlan

This command enables/disables VLAN in the switch. The value enable indicates that VLAN will be enabled in the device on all ports. The value disable indicates that VLAN will be disabled in the device on all ports.

`set vlan { enable | disable }`

Syntax Description	**`enable`**	-	Enables VLAN in the switch
	`disable`	-	Disables VLAN in the switch
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	enable		
Example	`switch(config)# set vlan enable`		

☞ The configuration can be set to disabled if and only if, GVRP and GMRP are disabled.

Related Commands

- **`show vlan`** - Displays VLAN information in the database
- **`show vlan device info`** - Displays the VLAN global status variables

7.2 Vlan

This command configures a VLAN in the switch and is also used to enter into the config-VLAN mode. The no form of the command deletes a VLAN from the switch.

vlan <vlan-id(1-4094)>

no vlan <vlan-id(1-4094)>

Mode	Global Configuration Mode . In Metro package, this command will be executed only in Switch configuration mode.
Package	Workgroup, Enterprise and Metro
Defaults	vlan-id - 1
Example	`switch(config)# vlan 4`

☞
- Leading zeros must not be entered for VLAN ID.
- The VLAN 1 interface cannot be deleted.
- This command is used in PBB bridge mode to create customer, service and backbone VLANs.

Related Command

show vlan - Displays VLAN information in the database

7.3 set mac-learning

This command configures the global mac learning status.

`set mac-learning { enable | disable }`

Syntax Description	**`enable`**	-	Enables the global mac learning status
	`disable`	-	Disables the global mac learning status

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	enable
Example	`switch(config)# set mac-learning enable`

7.4 set unicast-mac-learning

This command configures unicast-mac learning for the vlan

`set unicast-mac learning { enable | disable | default}`

Syntax Description	**`enable`**	-	Enables the unicast-mac learning for the vlan
	`disable`	-	Disables the unicast-mac learning for the vlan
	`default`	-	Sets the unicast-mac learning for the vlan as default

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Default	Enable
Example	`switch(config)# set unicast mac-learning enable`

7.5 clear vlan statistics

This command clears the VLAN counters.

`clear vlan statistics [vlan < vlan-id (1-4094)>]`

Syntax Description	**`vlan`**	**-**	VLAN Identifier
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config)# clear vlan statistics vlan 1`		

☞ If executed without the optional parameters this command clears all the VLAN counters.

Related Command

`show vlan statistics` - Displays the VLAN statistics

7.6 ports

This command configures a static VLAN entry with the required member ports, untagged ports and forbidden ports. The tagged and untagged member ports defined by this command are used for egress tagging for a VLAN at a port.

For ports in PBB bridge mode, this command is used to define member ports for a VLAN in a component.

- For BVLAN in a B component, these member ports can be only PNP.
- For SVLAN in an I component, these member ports can be only CNP-Stagged.
- For CVLAN in an I component, these member ports can be only CNP-Ctagged.

The no form of the command resets port list for the VLAN.

ports ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>]) [untagged <interface-type> <0/a-b,0/c,...> [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>][all])] [forbidden <interface-type> <0/a-b,0/c,...> [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>]] [name <vlan-name>]

no ports [<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>] [all] [untagged ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>] [all])] [forbidden ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>] [all])] [name <vlan-name>]

Syntax Description	**ports**	-	Member Ports Interface type and ID.
	<interface-type> <0/a-b, 0/c, ...>	-	Member Ports Interface type and Id.
	port-channel <a,b,c-d>	-	Port-channel ID
	untagged	-	Untagged Ports Interface type and Id
	<interface-type> <0/a-b, 0/c, ...>	-	Untagged Ports Interface type and Id
	forbidden	-	Forbidden Ports Interface type and Id
	<interface-type> <0/a-b, 0/c, ...>	-	Forbidden Ports Interface type and Id

port-channel - Port-channel ID

all - All Member Ports

name - Administratively assigned string used to identify the VLAN

Mode VLAN Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
switch(config-switch-vlan)# ports gigabitethernet 0/1 untagged
gigabitethernet 0/1 forbidden gigabitethernet 0/2 name vl1
```

- Member-ports represent the set of ports permanently assigned to the egress list
- Forbidden-ports represent the set of ports forbidden for the VLAN
- Untagged ports represent the set of ports which transmits untagged frames
- CBP should always be set as untagged member port of a BVLAN.
- All the existing commands in VLAN configuration mode are also used for the configuration of a B-VLAN of a PBB.

Related Command

show vlan - Displays VLAN information in the database

7.7 vlan active

This command makes the particular VLAN active in the switch.

`vlan active`

Mode	Config-VLAN Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config-vlan)# vlan active`

7.8 switchport pvid

This command configures the PVID (VLAN Identifier) on a port. The no form of this command sets the PVID to the default value on the port.

switchport pvid <vlan-id(1-4094)>

no switchport pvid

Syntax Description	**vlan-id**	-	PVID value to be configured on the port.
Mode	Interface Configuration Mode		
Example	`switch(config-if)# switchport pvid 3`		

☞

- If the frame (untagged/priority tagged/customer VLAN tagged) is received on a "tunnel" port, then the default Port VLAN Id (PVID) associated with the port is used.
- If the received frame cannot be classified as MAC-based or port-and-protocol-based, then the PVID associated with the port is used.
- For ports in PBB bridge mode, PVID can be configured on CNP and CBP.
- Usage is based on acceptable frame type of the port. Packets will be either dropped or accepted at ingress. Once a packet is accepted, if packet is having a tag, it will be processed against that tag. Otherwise, the packet will be processed against PVID.

Related Command

show vlan port config - Displays the VLAN related parameters specific for ports

7.9 switchport access vlan

This command configures the PVID (Port VLAN Identifier) on a port. The no form of this command sets the PVID to the default value on the port.

This command operates similar to that of the command switchport pvid.

switchport access vlan <vlanid (1-4094)>

no switchport access vlan

Syntax Description	**vlan-id**	-	PVID value to be configured on the port.
Mode	Interface Configuration Mode		
Example	`switch(config-if)# switchport access vlan 3`		

- If the frame (untagged/priority tagged/customer VLAN tagged) is received on a "tunnel" port, then the default PVID associated with the port is used.
- If the received frame cannot be classified as MAC-based or port-and-protocol-based, then the PVID associated with the port is used.
- For ports in PBB bridge mode, PVID can be configured on CNP (Customer Network Port) and CBP (Customer Backbone Port).
- Usage is based on acceptable frame type of the port. Packets will be either dropped or accepted at ingress. Once a packet is accepted, if the packet is having a tag, it will be processed against that tag. Otherwise, the packet will be processed against PVID.

Related Command

show vlan port config - Displays the VLAN related parameters specific for ports

7.10 switchport acceptable-frame-type

This command configures the acceptable frame type for the port. The no form of this command sets the default value of acceptable frame type - **all** where all frames will be accepted.

`switchport acceptable-frame-type {all | tagged | untaggedAndPrioritytagged }`

`no switchport acceptable-frame-type`

Syntax Description

`all` - All frames. Both tagged and untagged frames are allowed.

`tagged` - Tagged frames. For ports in PBB bridge mode, the description of tagged frames is given in the below table:

Port Type	What will be considered as TAG
CNP STagged	S-Tag
CNP CTagged	C-Tag
CNP Port Based	S-Tag
PIP	I-Tag
CBP	I-Tag
PNP	B-Tag or S Tag

`untaggedAndPrioritytagged` - Untagged and priority tagged frames. For ports in PBB bridge mode, the description of untagged frames is given in the below table:

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults all

Example

```
switch(config-if)# switchport acceptable-frame-type tagged
```

- When set to "tagged" the device will discard untagged and priority tagged frames received on the port and will process only the VLAN tagged frames
- When set to "all" untagged frames or priority-tagged frames received on the port are also accepted
- When set to “untaggedAndPrioritytagged”, untagged and priority tagged frames alone are accepted and tagged frames are dropped.

Related Command

`show vlan port config` - Displays the VLAN related parameters specific for ports.

7.11 switchport ingress-filter

This command enables ingress filtering on the port. The no form of this command disables ingress filtering on the port.

`switchport ingress-filter`

`no switchport ingress-filter`

Mode	Interface Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	Disabled
Example	`switch(config-if)# switchport ingress-filter`

☞
- When ingress-filtering is enabled, the device discards those incoming frames for VLANs which do not include this port in its member set
- When the ingress filtering is disabled using the no form of the command, the device accepts all incoming frames

Related Command

`show vlan port config` - Displays the VLAN related parameters specific for ports

7.12 port mac-vlan

This command enables MAC-based VLAN learning on the port. The no form of the command disables MAC-based VLAN learning on the port.

`port mac-vlan`

`no port mac-vlan`

Mode	Interface Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	Disabled
Example	`switch(config-if)# port mac-vlan`

☞ VLAN classification on the port will be MAC-based as long as MAC-based VLAN classification is enabled globally for the device.

Related Command

`show vlan port config` - Displays the VLAN related parameters specific for ports

7.13 port subnet – vlan

This command enables subnet based VLAN classification on the port. The no form of command disables the subnet based VLAN learning on the port.

`port subnet-vlan`

`no port subnet-vlan`

Mode	Interface Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	Disabled
Example	`switch(config-if)# port subnet-vlan`

Related Command

- **`show subnet vlan mapping`**: Displays the entries in Subnet-VLAN database

7.14 port protocol-vlan

This command enables port protocol based VLANs. The no form of the command disables port Protocol based VLANs.

`port protocol-vlan`

`no port protocol-vlan`

Mode	Interface Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	Enabled
Example	`switch(config-if)# port protocol-vlan`

☞ The value enable indicates that the VLAN classification on this port is port and protocol based as long as the port and protocol based classification is enabled globally for the device.

Related Command

`show vlan port config` - Displays the VLAN related parameters specific for ports

7.15 switchport map protocols-group

This command maps the protocol group configured to a particular VLAN identifier for the specified interface. The no form of the command unmaps the VLAN identifier to group Id mapping.

switchport map protocols-group <Group id integer(0-2147483647)>vlan <vlan-id(1-4094)>

no switchport map protocols-group <Group id integer(0-2147483647)>>

Syntax Description	**Group id**	-	Group ID
	vlan	-	VLAN ID
Mode	Interface Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config-if)# switchport map protocols-group 1 vlan 2`		

☞ Protocol group must have been configured

Related Commands

- Adds a protocol to a protocol group for protocol based VLAN learning
- **show protocol-vlan** - Displays the entries in protocol-VLAN database
- **show vlan protocols-group** - Displays the protocol group database

7.16 switchport priority default

This command sets the default user priority for the port. The no form of the command sets the default user priority for the port to the default value.

`switchport priority default <priority value(0-7)>`

`no switchport priority default`

Mode	Interface Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	0
Example	`switch(config-if)# switchport priority default 5`

Related Command

`show vlan port config` - Displays the VLAN related parameters specific for ports

7.17 switchport mode

This command configures the VLAN port mode. The no form of the command configures the default VLAN port mode.

`switchport mode { access | trunk | hybrid | {dynamic {auto | desirable}} }`

`no switchport mode`

Syntax Description	**`access`**	-	Access port Mode
	`trunk`	-	Trunk port Mode
	`hybrid`	-	Hybrid VLAN port Mode
	dynamic	-	Dynamic Mode. This can be: • auto – Interface converts the link to a trunk link. • desirable – Interface actively attempts to convert the link to a trunk link.
Mode	Interface Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	Hybrid Mode		
Example	`switch(config-if)# switchport mode access`		

☞
- It is not possible to set the switchport mode status to Trunk/Hybrid if the tunnel is enabled.
- It is not possible to configure the switchport mode status to trunk if the port is an untagged member of a VLAN.
- It is not possible to configure the switchport mode status to access if the ports acceptable frame type is All/Tagged.

Related Commands

- **`switchport mode dot1q-tunnel`** - Enables dot1q-tunneling on the specified interface
- **`show vlan port config`** - Displays the VLAN related parameters specific for ports

7.18 switchport mode dot1q-tunnel

This command enables dot1q-tunneling on the specified interface. The no form of the command disables dot1q-tunneling on the specified interface.

`switchport mode dot1q-tunnel`

`no switchport mode dot1q-tunnel`

Mode	Interface Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	Disabled
Example	`switch(config-if)# switchport mode dot1q-tunnel`

☞
- Bridge Mode must be set to 'provider' for the dot1q-tunneling status to be enabled
- It is not possible to set the dot1q-tunnel status on the port if the port mode is not 'access' type
- PNAC port control must be force-authorized
- If dot1q tunneling is enabled on the specified interface, then GMRP is disabled internally

Related Commands

- Configures the bridge mode of the Switch
- **`switchport mode`** - Configures the VLAN port mode
- **`show dot1q-tunnel`** - Displays the entries in the dot1q-tunnel table
- **`show vlan device info`** - Displays the VLAN related global status variables
- **`show vlan port config`** - Displays the VLAN port information

7.19 vlan max-traffic-class

This command configures the maximum number of traffic classes supported on a port. The no form of the command assigns the default maximum traffic class value to a port.

vlan max-traffic-class <MAX Traffic class(1-8)>

no vlan max-traffic-class

Syntax Description	**MAX Traffic class**	-	The number of traffic classes supported on the port
Mode	Interface Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	8		
Example	`switch(config-if)# vlan max-traffic-class 7`		

Related Command

show vlan traffic-classes - Displays the traffic classes information of all the available interfaces

7.20 debug vlan

This command sets the debug level. The no form of the command sets the debug level to default value.

debug vlan { global | [{fwd | priority | | redundancy} [initshut] [mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]] switch <context_name> }

no debug vlan { global | [{fwd | priority | | redundancy} [initshut] [mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]] switch <context_name> }

Syntax Description	**global**	-	Global related debug messages
	fwd	-	Forwarding Module
	priority	-	VLAN Priority Module
	redundancy		Redundancy related debug messages
	initshut	-	Init and Shutdown
	mgmt	-	Management
	data	-	Data path
	ctpl	-	Control Plane
	dump	-	Packet dump
	os	-	Traces related to all Resources except Buffer
	failall	-	All Failures
	buffer	-	Buffer
	all	-	All Traces

	switch	- Context/Switch Name. If the switch supports multiple instances, the name of the instance can be specified. Otherwise this parameter need not be given or the context name can be given as 'default'.

Mode	Privileged Exec Mode
Package	Workgroup, Enterprise and Metro
Defaults	Disabled
Example	`switch # debug vlan fwd all`

Related Command

Displays state of each debugging option

7.21 debug garp

This command sets debug level. The no form of the command sets the debug level to default value.

debug garp { global | [{protocol | gmrp | gvrp | redundancy} [initshut] [mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]] [switch <context_name>] }

no debug garp { global | [{protocol | gmrp | garp | redundancy} [initshut] [mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]] [switch <context_name>] }

Syntax Description	**global**	-	Global related debug messages
	protocol	-	Protocol related traces
	gmrp	-	GMRP related traces
	gvrp	-	GVRP related traces
	redundancy		Redundancy related debug messages
	initshut	-	Init and Shutdown
	mgmt	-	Management
	data	-	Data path
	ctpl	-	Control Plane
	dump	-	Packet dump
	os	-	Traces related to all Resources except Buffer
	failall	-	All Failures
	buffer	-	Buffer

all	-	All Traces
switch	-	Context/Switch Name. If the switch supports multiple instances, the name of the instance can be specified. Otherwise this parameter need not be given or the context name can be given as ‘default’

Mode	Privileged Exec Mode
Package	Workgroup, Enterprise and Metro
Defaults	Disabled
Example	`switch # debug garp fwd all`

Related Command

Displays state of each debugging option

7.22 show vlan

This command displays the VLAN information in the database.

show vlan [brief | id <vlan-range> | summary] [switch <context_name>]

Syntax Description	**brief**	-	Information about all the VLANs in brief
	id	-	Information specific to the VLAN Id
	summary	-	Summary of the VLAN
	switch	-	Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example

```
Single Instance:
switch# show vlan brief

Vlan database
-------------
Vlan ID        : 1
Member Ports   : Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5, Gi0/6
                 Gi0/7, Gi0/8, Gi0/9, Gi0/10, Gi0/11, Gi0/12
                 Gi0/13, Gi0/14, Gi0/15, Gi0/16, Gi0/17, Gi0/18
                 Gi0/19, Gi0/20, Gi0/21, Gi0/22, Gi0/23, Gi0/24
Untagged Ports   : Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5, Gi0/6
                 Gi0/7, Gi0/8, Gi0/9, Gi0/10, Gi0/11, Gi0/12
                 Gi0/13, Gi0/14, Gi0/15, Gi0/16, Gi0/17, Gi0/18
                 Gi0/19, Gi0/20, Gi0/21, Gi0/22, Gi0/23, Gi0/24
Forbidden Ports     : None
Name                :
Status              : Permanent
-----------------------------------------------------
switch# show vlan summary

Number of vlans : 1
```

Multiple Instance:

```
switch# show vlan
Switch - default

Vlan database
-------------
Vlan ID             : 1
Member Ports        : Gi0/49
Untagged Ports      : Gi0/49
Forbidden Ports     : None
Name                :
Status              : Permanent
-----------------------------------------------------

Switch - cust1

Vlan database
-------------
Vlan ID             : 1
Member Ports        : Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5, Gi0/6
Untagged Ports      : Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5, Gi0/6
Forbidden Ports     : None
Name                :
Status              : Permanent
-----------------------------------------------------
Vlan ID             : 20
Member Ports        : Gi0/1
Untagged Ports      : Gi0/1
Forbidden Ports     : None
Name                :
Status              : Permanent
-----------------------------------------------------
Vlan ID             : 30
Member Ports        : Gi0/2
Untagged Ports      : None
Forbidden Ports     : None
```

```
Name                  :
Status                : Dynamic Gvrp
------------------------------------------------------
```

☞ If the optional parameter is not specified then this command displays the VLAN information of all the available interfaces.

Related Commands

- Shuts down VLAN switching. The no form of the command starts and enables VLAN switching
- **`set vlan`** - Enables/disables VLAN in the switch
- **`vlan`** - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode
- **`ports`** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports

7.23 show vlan device info

This command displays the VLAN related global status variables.

show vlan device info [switch <context_name>]

Syntax Description	**switch**	-	Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example

Single Instance:

```
switch# show vlan device info

Vlan device configurations
--------------------------
Vlan Status                        : Enabled
Vlan Oper status                   : Enabled
Gvrp status                        : Enabled
Gmrp status                        : Disabled
Gvrp Oper status                   : Enabled
Gmrp Oper status                   : Disabled
Mac-Vlan Status                    : Disabled
Subnet-Vlan Status                 : Enabled
Protocol-Vlan Status               : Enabled
Bridge Mode                        : Customer Bridge
Base-Bridge Mode                   : Vlan Aware Bridge
Traffic Classes                    : Enabled
Vlan Operational Learning Mode     : IVL
Version number                     : 1
Max Vlan id                        : 4094
Max supported vlans                : 1024
Unicast mac learning limit         : 150
```

Multiple Instance:

```
switch# show vlan device info

Switch default

Vlan device configurations
--------------------------
Vlan Status                       : Enabled
Vlan Oper status                  : Enabled
Gvrp status                       : Enabled
Gmrp status                       : Enabled
Gvrp Oper status                  : Enabled
Gmrp Oper status                  : Enabled
Mac-Vlan Status                   : Disabled
Protocol-Vlan Status              : Enabled
Bridge Mode                       : Customer Bridge
Traffic Classes                   : Enabled
Vlan Operational Learning Mode    : IVL
Version number                    : 1
Max Vlan id                       : 4094
Max supported vlans               : 1024
Unicast mac learning limit        : 150
```

Related Commands

- Shuts down VLAN switching. The no form of the command starts and enables VLAN switching
- **`set vlan`** - Enables/disables VLAN in the switch
- **`vlan`** - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode
- - Enables MAC-based VLAN for all the available interfaces of the VLAN
- **`ports`** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports
- Enables or disables GVRP on a global basis
- Enables or disables GVRP on the interface
- Enables or disables GMRP on a global basis
- Enables or disables GMRP on the interface
- Enables or disables traffic classes
- **`vlan max-traffic-class`** - Assigns traffic class value to a port

- **`port protocol-vlan`** - Enables port protocol based VLANs
- Configures the VLAN learning mode
- **`show vlan traffic-classes`** - Displays the traffic classes information of all the available interfaces.
- **`show protocol-vlan`** - Displays the entries in the protocol-VLAN database.
- Sets unicast MAC learning limit for the switch

7.24 show vlan device capabilities

This command displays VLAN capabilities of the device.

show vlan device capabilities [switch <context_name>]

Syntax Description	**switch**	- Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	
Example	Single Instance: switch# show vlan device capabilities Vlan device capabilities --------------------------- Extended filtering services Traffic classes Static Entry Individual port IVL capable SVL capable Hybrid capable Configurable Pvid Tagging Multiple Instance: switch# show vlan device capabilities Switch - default Vlan device capabilities --------------------------- Extended filtering services Traffic classes Static Entry Individual port IVL capable SVL capable Hybrid capable	

```
Configurable Pvid Tagging

Switch - cust1
Vlan device capabilities
--------------------------

Extended filtering services
Traffic classes
Static Entry Individual port
IVL capable
SVL capable
Hybrid capable
Configurable Pvid Tagging
```

7.25 show fid - detail

This command displays forwarding database identifier used by VLANs in the switch.

show fid [<integer(1-4094)> | detail] [switch <context_name>]

Syntax Description	**switch**	-	Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example

```
Single Instance:
switch# show fid 2

Default Learning Type    : IVL
Fid Vlan mapping information
----------------------------
Fid     : 2
Vlan's  : 2,
----------------------------
switch# show fid detail

Default Learning Type    : IVL
Fid Vlan mapping information
----------------------------
Fid     : 1
Vlan's  : 1,
----------------------------
Fid     : 2
Vlan's  : 2,
----------------------------
Fid     : 3
Vlan's  : 3,
----------------------------
Fid     : 4
Vlan's  : 4,
```

```
----------------------------
Fid     : 5
Vlan's  : 5,
----------------------------
Fid     : 6
Vlan's  : 6,

Multiple Instance:
switch# show fid 2
Switch - default
Default Learning Type    : IVL

Fid Vlan mapping information
----------------------------
Fid     : 2
Vlan's  : 2,
----------------------------
Switch - cust1
Default Learning Type    : IVL

Fid Vlan mapping information
----------------------------
Fid     : 2
Vlan's  : 2,
----------------------------
```

Related Commands

- Configures a VLAN or a list of VLANs to use a Filtering database identified by a filtering database identifier
- Configures the default learning type for VLANs

7.26 show forward-all

This command displays the GMRP forward-all table entries.

show forward-all [switch <context_name>]

Syntax Description	**switch**	-	Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example

```
Single Instance:
switch# show forward-all

Vlan Forward All Table
------------------------

Vlan ID : 1
ForwardAll Ports          : Gi0/2
ForwardAll Static Ports   : Gi0/2
ForwardAll ForbiddenPorts : Gi0/1
------------------------------------------------------------
Vlan ID : 2
ForwardAll Ports          : Gi0/1
ForwardAll Static Ports   : Gi0/1
ForwardAll ForbiddenPorts : Gi0/2
------------------------------------------------------------

Multiple Instance:

switch# show forward-all

Switch – default

Vlan Forward All Table
------------------------
```

```
Vlan ID : 1
ForwardAll Ports          : Gi0/2
ForwardAll Static Ports   : Gi0/2
ForwardAll ForbiddenPorts : Gi0/1
------------------------------------------------------------
Vlan ID : 2
ForwardAll Ports          : Gi0/1
ForwardAll Static Ports   : Gi0/1
ForwardAll ForbiddenPorts : Gi0/2
------------------------------------------------------------
```

Related Commands

- **`vlan`** - Configures a VLAN in the switch and is used to enter into the VLAN mode
- **`ports`** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports
- Configures the forward-all information for a VLAN

7.27 show forward-unregistered

This command displays the GMRP forward-unregistered table.

show forward-unregistered [switch <context_name>]

Syntax Description	**switch**	-	Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example

```
Single Instance:
switch# show forward-unregistered

Vlan Forward Unregistered Table
---------------------------------


Vlan ID : 1
Unreg ports           : Gi0/1
Unreg Static Ports    : Gi0/1
Unreg Forbidden Ports : Gi0/2
-------------------------------------------------------
Vlan ID : 2
Unreg ports           : Gi0/2
Unreg Static Ports    : Gi0/2
Unreg Forbidden Ports : Gi0/1
-------------------------------------------------------

Multiple Instance:
switch# show forward-unregistered

Switch - default


Vlan Forward Unregistered Table
---------------------------------
```

```
Vlan ID : 1
Unreg ports           : Gi0/49
Unreg Static Ports    : Gi0/49
Unreg Forbidden Ports : None
-----------------------------------------------------


Switch - cust1


Vlan Forward Unregistered Table
--------------------------------


Vlan ID : 1
Unreg ports            : Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5,
Gi0/6
Unreg Static Ports     : Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5,
Gi0/6
Unreg Forbidden Ports : None
-----------------------------------------------------
Vlan ID : 20
Unreg ports           : Gi0/1
Unreg Static Ports    : Gi0/1
Unreg Forbidden Ports : None
-----------------------------------------------------
Vlan ID : 30
Unreg ports           : Gi0/2
Unreg Static Ports    : Gi0/2
Unreg Forbidden Ports : None
-----------------------------------------------------
```

Related Commands

- **`vlan`** - Configures a VLAN in the switch and is used to enter into the VLAN mode
- **`ports`** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports
- Configures the forward unregistered information for a VLAN

7.28 show vlan traffic-classes

This command displays the traffic classes information of all the available interfaces.

show vlan traffic-classes [{port <interface-type> <interface-id> | switch <context_name>}]

Syntax Description	**port**	-	Interface Type and ID of the port
	switch	-	Context/Switch Name. This parameter is specific to Multiple Instance.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
Single Instance:
switch# show vlan traffic-classes

Traffic Class table
---------------------
Port     Priority    Traffic Class
-----    ---------   -------------
Gi0/1    0           2
Gi0/1    1           0
Gi0/1    2           1
Gi0/1    3           3
Gi0/1    4           4
Gi0/1    5           5
Gi0/1    6           6
Gi0/1    7           7
Gi0/2    0           2
Gi0/2    1           0
Gi0/2    2           1
Gi0/2    3           3
Gi0/2    4           4
Gi0/2    5           5
```

```
Gi0/2    6           6
Gi0/2    7           7
```

Multiple Instance:

```
switch# show vlan traffic-classes

Switch - default

Traffic Class table
---------------------
Port     Priority    Traffic Class
-----    ---------   -------------
Gi0/49    0           2
Gi0/49    1           0
Gi0/49    2           1
Gi0/49    3           3
Gi0/49    4           4
Gi0/49    5           5
Gi0/49    6           6
Gi0/49    7           7

Switch - cust1

Traffic Class table
---------------------
Port     Priority    Traffic Class
-----    ---------   -------------
Gi0/1    0           2
Gi0/1    1           0
Gi0/1    2           1
Gi0/1    3           3
Gi0/1    4           4
Gi0/1    5           5
Gi0/1    6           6
Gi0/1    7           7
Gi0/2    0           2
Gi0/2    1           0
Gi0/2    2           1
```

```
Gi0/2     3            3
Gi0/2     4            4
Gi0/2     5            5
Gi0/2     6            6
Gi0/2     7            7
```

☞ If executed without the ports option, this command displays the priority mapped to all the available traffic classes on the port.

Related Commands

- **`vlan`** - Configures a VLAN in the switch and is used to enter into the VLAN mode
- **`ports`** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports
- Enables / disables traffic classes
- **`vlan max-traffic-class`** - Assigns traffic class value to a port

7.29 show vlan port config

This command displays the VLAN related parameters specific for ports.

show vlan port config [{port <interface-type> <interface-id> | switch <context_name>}]

Syntax Description	**port**	-	Interface type and ID of the port
	switch	-	Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example

```
Single Instance:
switch# show vlan port config

Vlan Port configuration table
------------------------------
Port Gi0/1
 Port Vlan ID                       : 1
 Port Acceptable Frame Type         : Admit All
 Port Ingress Filtering             : Disabled
 Port Mode                          : Hybrid
 Port Gvrp Status                   : Enabled
 Port Gmrp Status                   : Enabled
 Port Gvrp Failed Registrations     : 0
 Gvrp last pdu origin               : 00:00:00:00:00:00
 Port Restricted Vlan Registration  : Disabled
 Port Restricted Group Registration : Disabled
 Mac Based Support                  : Disabled
 Subnet Based Support               : Disabled
 Port-and-Protocol Based Support    : Enabled
 Default Priority                   : 0
 Filtering Utility Criteria         : Default
 Port Protected Status              : Disabled
```

```
 ------------------------------------------------------
Port Gi0/2
 Port Vlan ID                        : 1
 Port Acceptable Frame Type          : Admit All
 Port Ingress Filtering              : Disabled
 Port Mode                           : Hybrid
 Port Gvrp Status                    : Enabled
 Port Gmrp Status                    : Enabled
 Port Gvrp Failed Registrations      : 0
 Gvrp last pdu origin                : 00:00:00:00:00:00
 Port Restricted Vlan Registration   : Disabled
 Port Restricted Group Registration  : Disabled
 Mac Based Support                   : Disabled
 Subnet Based Support                : Disabled
 Port-and-Protocol Based Support     : Enabled
 Default Priority                    : 0
 Filtering Utility Criteria          : Default
 Port Protected Status               : Disabled
 ------------------------------------------------------
```

Multiple Instance:

```
switch# show vlan port config

Switch - default


Vlan Port configuration table
-------------------------------
Port Gi0/49
 Port Vlan ID                        : 1
 Port Acceptable Frame Type          : Admit All
 Port Ingress Filtering              : Disabled
 Port Mode                           : Hybrid
 Port Gvrp Status                    : Enabled
 Port Gmrp Status                    : Enabled
 Port Gvrp Failed Registrations      : 0
 Gvrp last pdu origin                : 00:00:00:00:00:00
 Port Restricted Vlan Registration   : Disabled
 Port Restricted Group Registration  : Disabled
 Mac Based Support                   : Disabled
```

```
 Port-and-Protocol Based Support     : Enabled
 Default Priority                    : 0
 Dot1x Protocol Tunnel Status        : Peer
 LACP Protocol Tunnel Status         : Peer
 Spanning Tree Tunnel Status         : Peer
 GVRP Protocol Tunnel Status         : Peer
 GMRP Protocol Tunnel Status         : Peer
 IGMP Protocol Tunnel Status         : Peer
 Filtering Utility Criteria          : Enhanced
 ---------------------------------------------------

Switch - cust1

Vlan Port configuration table
-------------------------------
Port Gi0/1
 Port Vlan ID                        : 20
 Port Acceptable Frame Type          : Admit All
 Port Ingress Filtering              : Disabled
 Port Mode                           : Hybrid
 Port Gvrp Status                    : Enabled
 Port Gmrp Status                    : Enabled
 Port Gvrp Failed Registrations      : 0
 Gvrp last pdu origin                : 00:00:00:00:00:00
 Port Restricted Vlan Registration   : Disabled
 Port Restricted Group Registration  : Disabled
 Mac Based Support                   : Disabled
 Port-and-Protocol Based Support     : Enabled
 Default Priority                    : 0
 ---------------------------------------------------
Port Gi0/2
 Port Vlan ID                        : 1
 Port Acceptable Frame Type          : Admit All
 Port Ingress Filtering              : Disabled
 Port Mode                           : Hybrid
 Port Gvrp Status                    : Enabled
 Port Gmrp Status                    : Enabled
```

```
Port Gvrp Failed Registrations      : 0
Gvrp last pdu origin                : 00:01:02:03:04:0e
Port Restricted Vlan Registration   : Disabled
Port Restricted Group Registration  : Disabled
Mac Based Support                   : Disabled
Port-and-Protocol Based Support     : Enabled
Default Priority                    : 0
-----------------------------------------------------
```

☞ If executed with out the optional parameter this command displays the port information of all the available ports.

Related Commands

- Enables or disables GVRP on the interface
- Enables or disables GMRP on the interface
- **`switchport pvid / switchport access vlan`** - Configures the PVID (VLAN ID) that would be assigned to untagged/priority-tagged frames/VLAN tagged frames
- **`switchport acceptable-frame-type`** - Configures the acceptable frame type for the port
- **`switchport ingress-filter`** - Enables ingress filtering on the port
- **`port mac-vlan`** - Enables MAC-based VLAN on the port
- **`port protocol-vlan`** - Enables port protocol based VLANs
- Enables/disables restricted VLAN registration on the port

7.30 show vlan protocols-group

This command displays the protocol group database.

show vlan protocols-group [switch <context_name>]

Syntax Description	**switch**	-	Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example

```
Single Instance:
switch# show vlan protocols-group

Protocol Group Table
--------------------
-----------------------------------------
Frame Type      Protocol            Group
-----------------------------------------
Enet-v2         IP                  1
Snap            Novell              2
-----------------------------------------

Multiple Instance:

switch# show vlan protocols-group

Switch - default

Protocol Group Table
--------------------
-----------------------------------------
Frame Type      Protocol            Group
-----------------------------------------
Enet-v2         IP                  1
Snap            Novell              2
-----------------------------------------
```

Related Commands

- Configures the group ID for a specific encapsulation and protocol value combination
- **`show protocol-vlan`** - Displays the entries in the protocol-VLAN database
- **`switchport map protocols-group`** - Maps the protocol group configured to a particular VLAN identifier for the specified interface

7.31 show protocol-vlan

This command displays the entries in protocol-VLAN database.

`show protocol-vlan [ switch <context_name>]`

Syntax Description	**`switch`**	-	Context/Switch Name. This parameter is specific to Multiple Instance.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
Single Instance:
switch# show protocol-vlan

Port Protocol Table
---------------------------------------
Port           Group          Vlan ID
---------------------------------------
Gi0/2          1              2
Gi0/1          2              3
---------------------------------------


Multiple Instance:
switch# show protocol-vlan

Switch - default

Port Protocol Table
---------------------------------------
Port           Group          Vlan ID
---------------------------------------
```

```
Gi0/2          1              2
Gi0/1          2              3
---------------------------------------
```

Related Command

`switchport map protocols-group` - Maps the protocol group configured to a particular VLAN identifier for the specified interface

7.32 show mac-vlan

This command displays the entries in the MAC-VLAN database.

`show mac-vlan [{interface <interface-type> <interface-id>] [ switch <context_name>]`

Syntax Description	**`interface`**	-	Interface Type and Identifier
	`switch`	-	Context/Switch Name. This parameter is specific to Multiple Instance.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
Single Instance:
switch# show mac-vlan interface gigabitethernet 0/1
     Mac Map Table For Port 1--Mac Vlan Disabled
     --------------------------

     Mac Address        Vlan ID          MCast/Bcast
     -----------        -------          -----------
     00:11:11:11:11:11    1              discard
     00:22:22:22:22:22    1              allow

Multiple Instance:
switch# show mac-vlan switch cust1

Switch - cust1
```

```
Mac Map Table
--------------
Mac Address         Vlan ID
-----------         -------
00:11:22:33:44:55   2
```

Related Commands

- Enables MAC-based VLAN for all the available interfaces of the VLAN
- Configures the VLAN-MAC address mapping
- **`show vlan device info`** - Displays the VLAN global status variables

7.33 show subnet vlan mapping

This command displays the entries in Subnet-VLAN database.

`show subnet-vlan mapping [{interface <interface-type> <interface-id> | switch <string(32)>}]`

Syntax Description	**`interface`**	-	Interface Type and Identifier
	`switch`	-	Context/Switch Name. This parameter is specific to Multiple Instance.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
switch# show subnet -vlan mapping interface gigabitethernet 0/1

Subnet Map Table For Port 1--Subnet Vlan Enabled
------------------------------------------------
Subnet Address      Vlan ID        ARP Traffic
------------------------------------------------
14.0.0.0            1              allow
192.168.1.0         1              discard
```

7.34 show vlan counters

This command displays the VLAN counters database.

show vlan counters [vlan <vlan-range>] [switch <context_name>]

Syntax Description	**vlan**	-	VLAN range.
	switch	-	Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example

```
Single Instance:
switch# show vlan counters

Port Vlan statistics
--------------------------
Port Gi0/1
 Vlan ID    : 1
 In frames  : 342
 Out frames : 345
 Discards   : 0
Port Gi0/1
 Vlan ID    : 2
 In frames  : 446
 Out frames : 248
 Discards   : 0
Port Gi0/2
 Vlan ID    : 2
 In frames  : 115
 Out frames : 517
 Discards   : 7
Port Gi0/2
```

```
 Vlan ID    : 2
 In frames  : 0
 Out frames : 0
 Discards   : 0
Multiple Instance:
switch# show vlan counters
Switch - default

Port Vlan statistics
--------------------------
Port Gi0/49
 Vlan ID    : 1
 In frames  : 75
 Out frames : 0
 Discards   : 0
--------------------------

Switch - cust1

Port Vlan statistics
--------------------------
Port Gi0/1
 Vlan ID    : 1
 In frames  : 0
 Out frames : 0
 Discards   : 0
--------------------------
Port Gi0/1
 Vlan ID    : 20
 In frames  : 0
 Out frames : 0
 Discards   : 0
--------------------------
Port Gi0/2
 Vlan ID    : 1
 In frames  : 70
 Out frames : 0
```

```
 Discards   : 0
---------------------------
Port Gi0/2
 Vlan ID    : 30
 In frames  : 0
 Out frames : 0
 Discards   : 2
---------------------------
```

Related Commands

- **`vlan`** - Configures a VLAN in the switch and is also used to enter into the config-VLAN mode
- **`ports`** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports

7.35 show vlan statistics

This command displays VLAN statistics such as the number of unicast frames forwarded broadcast packets and unknown unicast packets flooded in that VLAN.

show vlan statistics [vlan <vlan-range>] [switch <context_name>]

Syntax Description	**vlan**	- VLAN range.
	switch	- Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	

Example

```
Single Instance
switch# show vlan statistics vlan 1

Unicast/broadcast Vlan statistics
-------------------------------------
 Vlan Id                          : 1
 Unicast frames received          : 0
 Mcast/Bcast frames received      : 0
 Unknown Unicast frames flooded   : 0
 Unicast frames transmitted       : 0
 Broadcast frames transmitted     : 0
-------------------------------------
Multiple Instance

switch# show vlan statistics vlan 1 switch sw1

          Switch – sw1


          Unicast/broadcast Vlan statistics
          -------------------------------------
          Vlan Id                          : 1
          Unicast frames                   : 16
          Broadcast frames                 : 10
          Unicast frames flooded           : 25
          -------------------------------------
```

☞ If VLAN ID is not specified in the command, statistics of all the VLAN existing in the system will be displayed.

Related Command

`clear vlan statistics` - Clears the VLAN counters

7.36 show mac-address-table

This command displays the static and dynamic unicast and multicast MAC address table.

`show mac-address-table [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [interface <interface-type> <interface-id> ]`

Syntax Description	**`vlan`**	-	VLAN range
	`address`	-	MAC address
	`interface`	-	Interface type and ID
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example

```
switch# show mac-address-table vlan 2

Vlan    Mac Address         Type      ConnectionId       Ports
----    -----------         ----      ------------       -----
2       00:01:02:03:04:21   Learnt                       Gi0/1

Total Mac Addresses displayed: 1

switch# show mac-address-table interface gigabitethernet 0/1

Vlan    Mac Address         Type      ConnectionId       Ports
----    -----------         ----      ------------       -----
2       00:01:02:03:04:21   Learnt                       Gi0/1
1       01:02:03:04:05:06   Static                       Gi0/1

Total Mac Addresses displayed: 2
```

☞ If executed without the optional parameters this command displays all the static and dynamic MAC entries

Related Commands

- **`vlan`** - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode
- **`ports`** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports
- Configures a static unicast MAC address in the forwarding database
- Configures a static multicast MAC address in the forwarding database

7.37 show mac-address-table count

This command displays the number of MAC addresses present on all the VLANs or on the specified VLAN.

`show mac-address-table count [vlan <vlan-id(1-4094)>] [ switch <context_name>]`

Syntax Description	**`vlan`**	-	VLAN ID
	`switch`	-	Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example	Single Instance
	`switch# show mac-address-table count`
	`Mac Entries for Vlan 1:`
	`---------------------------`
	`Dynamic Unicast Address Count : 1`
	`Dynamic Multicast Address Count : 0`
	`Static Unicast Address Count : 1`
	`Static Multicast Address Count : 1`
	`----------------------------------------`		

```
Mac Entries for Vlan 2:
--------------------------
Dynamic Unicast Address Count    : 1
Dynamic Multicast Address Count  : 0
Static Unicast Address Count     : 1
Static Multicast Address Count   : 0
---------------------------------------
```

Multiple Instance:

```
switch# show mac-address-table count switch cust1

Switch - cust1


Mac Entries for Vlan 1:
--------------------------
Dynamic Unicast Address Count    : 1
Dynamic Multicast Address Count  : 0
Static Unicast Address Count     : 0
Static Multicast Address Count   : 0
---------------------------------------


Mac Entries for Vlan 20:
--------------------------
Dynamic Unicast Address Count    : 0
Dynamic Multicast Address Count  : 0
Static Unicast Address Count     : 0
Static Multicast Address Count   : 0
---------------------------------------


Mac Entries for Vlan 30:
--------------------------
Dynamic Unicast Address Count    : 0
Dynamic Multicast Address Count  : 0
Static Unicast Address Count     : 0
Static Multicast Address Count   : 0
---------------------------------------
```

☞ If executed without the optional parameter this command displays the MAC addresses present on all the VLANs.

Related Commands

- **vlan** - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode
- **ports** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports
- **C**onfigures a static unicast MAC address in the forwarding database
- Configures a static multicast MAC address in the forwarding database

7.38 show mac-address-table static unicast

This command displays the statically configured unicast addresses from the MAC address table.

show mac-address-table static unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> | switch <context_name>}]

Syntax Description	**vlan**	-	VLAN Id
	address	-	MAC address
	interface	-	Interface type and ID
	switch	-	Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example

Single Instance:

```
switch# show mac-address-table static unicast
Vlan  Mac Address        RecvPort  Status   ConnectionId  Ports


----  -----------        -------- ------      -----      -------
2     00:11:22:33:44:55   Gi0/2   Del-OnTimeout           Gi0/3
```

Multiple Instance:

```
switch# sh mac-address-table static unicast switch cust1
Switch - cust1


Vlan  Mac Address        SrvInst/ Status         Ports
----  -----------        -------- ------         -----
1     00:11:22:33:44:55   Gi0/2   Permanent      Gi0/3


Total Mac Addresses displayed: 1
```

☞ If executed without the optional parameters this command displays the MAC address table for all the available interfaces.

Related Commands

- **vlan** - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode
- **ports** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports
- Configures a static unicast MAC address in the forwarding database
- **show mac-address-table dynamic unicast** - Displays the dynamic MAC address table for the specified address or for all the addresses

7.39 show mac-address-table static multicast

This command displays the statically configured multicast entries.

show mac-address-table static multicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> | switch <context_name>}]

Syntax Description	**vlan**	-	VLAN Id
	address	-	MAC address

	interface	-	Interface type and ID
	switch	-	Context/Switch Name. This parameter is specific to Multiple Instance.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

Single Instance:

```
switch# show mac-address-table static multicast

Static Multicast Table
----------------------
Vlan            : 1
Mac Address     : 01:02:03:04:05:06
Receive Port    : Gi0/1
Member Ports    : Gi0/1
Forbidden Ports : Gi0/2
Status          : Permanent
-------------------------------------------------

Total Mac Addresses displayed: 1
```

Multiple Instance:

```
switch# sh mac-address-table static multicast switch cust1
Switch - cust1

Static Multicast Table
----------------------
Vlan            : 1
Mac Address     : 01:02:03:04:05:06
Receive Port    : Gi0/2
Member Ports    : Gi0/3

Status          : Permanent
-------------------------------------------------
```

```
Total Mac Addresses displayed: 1
```

Related Commands

- **vlan** - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode
- **ports** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports
- Configures a static multicast MAC address in the forwarding database
- **show mac-address-table dynamic multicast** - Displays the dynamic MAC address table for the specified address or for all the addresses

7.40 show mac-address-table dynamic unicast

This command displays the dynamically learnt unicast entries from the MAC address table.

show mac-address-table dynamic unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> | switch <context_name>}]

Syntax Description	**vlan**	-	VLAN Id
	address	-	MAC address
	interface	-	Interface type and ID
	switch	-	Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example

```
Single Instance:
switch# show mac-address-table dynamic unicast vlan 2

Vlan    Mac Address         Type     ConnectionId  Ports
----    -----------         ----     ------------  -----
2       00:01:02:03:04:21   Learnt                 Gi0/1
```

```
Total Mac Addresses displayed: 1

Multiple Instance:
switch# show mac-address-table dynamic unicast

Switch - default

Vlan    Mac Address          Type     Ports
----    -----------          ----     -----
1       00:02:02:03:04:04    Learnt   Gi0/2
1       00:03:02:03:04:04    Learnt   Gi0/3
2       00:02:02:03:04:04    Learnt   Gi0/2
2       00:03:02:03:04:04    Learnt   Gi0/3
3       00:02:02:03:04:04    Learnt   Gi0/2
3       00:03:02:03:04:04    Learnt   Gi0/3

Total Mac Addresses displayed: 6
```

☞ If executed without the optional parameters this command displays the MAC address table of all the available interfaces

Related Commands

- **`vlan`** - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode
- **`ports`** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports
- Configures a static unicast MAC address in the forwarding database
- **`show mac-address-table static unicast`** - Displays the statically configured unicast address from the MAC address table

7.41 show mac-address-table dynamic multicast

This command displays the dynamically learnt multicast MAC address.

show mac-address-table dynamic multicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> | switch <context_name>}]

Syntax Description	**vlan**	-	VLAN Id
	address	-	MAC address
	interface	-	Interface type and ID
	switch	-	Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example

Single Instance:

```
switch# show mac-address-table dynamic multicast

Vlan    Mac Address         Type     ConnectionId Ports
----    -----------         ----     ------------ -----
2       01:03:05:07:09:04   Learnt                Gi0/1

Total Mac Addresses displayed: 1
```

Multiple Instance:

```
switch# show mac-address-table dynamic multicast

Switch - default

Vlan    Mac Address         Type     Ports
----    -----------         ----     -----
```

```
2       01:02:02:02:02:02   Learnt   Gi0/2, Gi0/3
3       01:02:02:02:02:02   Learnt   Gi0/2
3       01:03:03:03:03:03   Learnt   Gi0/3

Total Mac Addresses displayed: 3
```

☞ If executed without the optional parameters this command displays the MAC address table of all the available interfaces.

Related Commands

- **`vlan`** - Configures a VLAN in the switch and is also used to enter into the config-VLAN mode
- **`ports`** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports
- Configures a static multicast MAC address in the forwarding database
- **`show mac-address-table static multicast`** - Displays the statically configured multicast entries

7.42 show mac-address-table aging-time

This command displays the MAC address-table ageing time.

`show mac-address-table aging-time [ switch <context_name>]`

Syntax Description	**`switch`**	-	Context/Switch Name. This parameter is specific to Multiple Instance.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example

Single Instance:

```
switch# show mac-address-table aging-time

Mac Address Aging Time: 300
```

Multiple Instance:

```
switch# show mac-address-table aging-time

Context default: Mac Address Aging Time: 300
```

Related Commands

- **`show mac-address-table`** - Displays the static and dynamic MAC entries
- Configures the MAC address table entry maximum age

Chapter 8

8.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

8.1 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		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config)# monitor session 1 source interface extreme-ethernet 0/1 rx`		

8.2 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
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# monitor session 1 destination interface extreme-ethernet 0/2`

Chapter 9

9. SNMP v3

SNMP (Simple Network Management Protocol) is the most widely-used network management protocol on TCP/IP-based networks. SNMPv3 is designed mainly to overcome the security shortcomings of SNMPv1/v2. USM (User based Security Model) and VACM (View based Access Control Model) are the main features added as part of the SNMPv3 specification. USM provides for both encryption and authentication of the SNMP PDUs, while VACM specifies a mechanism for defining access policies for different users with different MIB trees. Also, SNMPv3 specifies a generic management framework, which is expandable for adding new Management Engines, Security Models, Access Control Models and so on. With SNMPv3, the SNMP communication is completely safe and secure.

SNMPv3 is a multi-lingual Agent supporting all three versions of SNMP (SNMPv1, SNMPv2c and SNMPv3) while conforming to the latest specifications. It is available as a portable source code product, which can be easily integrated to any platform (any OS and any Processor). MIB integration is made simple with the aid of a tool called Middle Level Code Generator (MIDGEN), which is available along with **Garland Technology SNMP**. MIDGEN generates the interface stubs required for every object in the MIB for the SET, GET and GETNEXT operations.

These stubs can be implemented by the respective modules supporting the MIB. **Garland Technology SNMP** is provided as source code available for licensing to OEMs and VARs.

The list of CLI commands for the configuration of SNMPv3 is as follows:

- enable snmpsubagent
- disable snmpsubagent
- show snmp agentx information
- show snmp agentx statistics
- enable snmpagent
- disable snmpagent
- snmp community index
- snmp group
- snmp access

- snmp engineid
- snmp proxy name
- snmp mibproxy name
- snmp view
- snmp targetaddr
- snmp targetparams
- snmp user
- snmp notify
- snmp filterprofile
- snmp-server enable traps snmp authentication
- snmp-server trap udp-port
- snmp-server trap proxy-udp-port
- snmp agent port
- snmp tcp enable
- snmp trap tcp enable
- snmp-server tcp-port
- snmp-server trap tcp-port
- snmp-server enable traps
- show snmp
- show snmp community
- show snmp group
- show snmp group access
- show snmp engineID
- show snmp proxy
- show snmp mibproxy
- show snmp viewtree
- show snmp targetaddr
- show snmp targetparam
- show snmp user
- show snmp notif
- show snmp inform statistics
- show snmp-server traps
- show snmp-server proxy-udp-port
- show snmp tcp
- show snmp filter table

9.1 enable snmpsubagent

This command enables either snmp agent or agentx-subagent capabilities.

enable snmpsubagent { master { ip4 <ipv4_address> | ip6 <ipv6_address> } [port <number>] }

Syntax Description	**snmpsubagent**	-	Enables SNMP Subagent
	master	-	The master agent address. It can be either ip4 or ip6.
	port	-	Port number on which master agent listens subagent.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	port	-	705
Example	`switch(config)# enable snmpsubagent master ip4 10.0.0.5 port 897`		

Related Commands

- **show snmp agentx information** - Displays global information of SNMP Agentx communications.
- **show snmp agentx statistics** - Displays all the information regarding SNMP Agentx statistics.

9.2 disable snmpsubagent

This command disables agentx-subagent.

`disable snmpsubagent`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# disable snmpsubagent`

Related Commands

- **`show snmp agentx information`** - Displays global information of SNMP Agentx communications.
- **`show snmp agentx statistics`** - Displays all the information regarding SNMP Agentx statistics.

9.3 show snmp agentx information

This command displays global information of SNMP Agentx communications.

show snmp agentx information

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show snmp agentx information`

```
Agentx Subagent is enabled
TransportDomain   :TCP
Master IP Address :10.0.0.2
Master PortNo     :705
```

9.4 show snmp agentx statistics

This command displays all the information regarding SNMP Agentx statistics.

show snmp agentx statistics

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
switch# show snmp agentx statistics

Tx Statistics
  Transmitted Packets               :860
  Open PDU                          :1
  Index Allocate PDU                :0
  Index DeAllocate PDU              :0
  Register PDU                      :2
  Add Agent Capabilities PDU        :0
  Notify PDU                        :0
  Ping PDU                          :20
  Remove Agent Capabilities PDU     :0
  UnRegister PDU                    :0
  Close PDU                         :0
  Response PDU                      :837

Rx Statistics
  Rx Packets                        :859
  Get PDU                           :1
  GetNext PDU                       :836
  GetBulk PDU                       :0
  TestSet PDU                       :0
  Commit PDU                        :0
  Cleanup PDU                       :0
  Undo PDU                          :0
```

```
Dropped Packets                 :0
Parse Drop Errors               :1
Open Fail Errors                :0
Close PDU                       :0
Response PDU                    :21
```

9.5 enable snmpagent

This command enables SNMP agent.

`enable snmpagent`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	SNMP agent is enabled.
Example	`switch(config)# enable snmpagent`

Related Commands

- **`disable snmpagent`** - Disables SNMP agent.
- **`enable snmpsubagent`** - Enables either snmp agent or agentx-subagent capabilities.

9.6 disable snmpagent

This command disables SNMP agent.

`disable snmpagent`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# disable snmpagent`

Related Commands

- **`enable snmpagent`** - Enables SNMP agent.
- **`enable snmpsubagent`** - Enables either snmp agent or agentx-subagent capabilities.

9.7 snmp community index

This command configures the SNMP community details. The no form of this command removes the SNMP community details.

snmp community index <CommunityIndex> name <CommunityName> security <SecurityName> [context <Name >] [{volatile | nonvolatile}] [transporttag <TransportTagIdentifier | none>] [contextengineid <ContextEngineID>]

no snmp community index <CommunityIndex>

Syntax Description	**CommunityIndex**	-	Community index identifier
	name	-	Community name
	security	-	User Name
	context	-	Context name through which the management information is accessed when using the community string specified by the corresponding instance of SNMP community name
	volatile | nonvolatile	-	Storage type
	transporttag	-	Transport tag identifier
	contextengineid		Context engine identifier.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	Community Index	-	NETMAN/PUBLIC
	CommunityName	-	NETMAN/PUBLIC
	Security Name	-	None

ContextName	-	Null
Transport Tag	-	Null
Storage type	-	Volatile

Example

```
switch(config)# snmp community index myv3com name myv3com
security xyz context myinst nonvolatile transporttag myv3tag
```

☞ The community index identifier must be unique for every community name entry.

Related Commands

- **`show snmp`** - Displays the status information of SNMP communications
- **`show snmp community`** - Displays the configured SNMP community details

9.8 snmp group

This command configures SNMP group details. The no form of the command removes the SNMP group details.

snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3 } [{volatile | nonvolatile}]

no snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3 }

Syntax Description	**GroupName**	-	Name of the SNMP group
	user	-	User Name
	security-model	-	Security Model
	volatile | nonvolatile	-	Storage Type
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	Group Name	-	iso/initial

Example

```
switch(config)# snmp group myv3group user myv3user
security-model v1 volatile
```

Related Commands

- **show snmp group** - Displays the configured SNMP groups
- **show snmp user** - Displays the configured SNMP users

9.9 snmp access

This command configures the SNMP group access details. The no form of the command removes the SNMP group access details.

snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}} [read <ReadView | none>] [write <WriteView | none>] [notify <NotifyView | none>] [{volatile | nonvolatile}] [context <name>]

no snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}} [context <name>]

Syntax Description	**GroupName**	-	Name of the group
	v1 | v2c | v3	-	Version of the SNMP
	auth	-	Authentication - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication
	noauth	-	no-authentication
	priv	-	Specifies both authentication and privacy
	read	-	A read view identifier
	write	-	A write view identifier
	notify	-	A notification view identifier
	volatile | nonvolatile	-	Storage type
	context	-	Name of the SNMP context
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		

Defaults	Group Name		-	iso
	Read/Write/Notify	view	-	iso
	Storage Type		-	volatile
	Group Name		-	initial
	Read/Write/Notify	View	-	restricted
	Storage Type		-	non-volatile
	Group Name		-	initial
	Read/Write/Notify	View	-	iso
	Storage Type		-	non-volatile

Example

```
switch(config)# snmp access myv2group v2 read v2readview write
v2writeview notify v2notifyview nonvolatile
```

- To configure an SNMP access along with the group, a group must have already been created using the snmp group command
- Version 3 is the most secure model as it allows packet encryption with the priv key word

Related Commands

- **`snmp group`** - Configures SNMP group details
- **`snmp view`** - Configures the SNMP view
- **`show snmp group`** - Displays the configured SNMP groups
- **`show snmp group access`** - Displays the configured SNMP group access details
- **`show snmp viewtree`** - Displays the configured SNMP Tree views

9.10 snmp engineid

This command configures the engine identifier. The no form of the command removes the configured engine identifier.

snmp engineid <EngineIdentifier>

no snmp engineid

Syntax Description	**EngineIdentifier**	-	Engine ID
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	80.00.08.1c.04.46.53		
Example	`switch(config)# snmp engineid 80.0.08.1c.04.5f.a9`		

☞

- The Engine ID must be given as octets in hexadecimal separated by dots and the allowed length is 5 to 32 octets.
- SNMP engine ID is an administratively unique identifier.
- Changing the value of the SNMP engine ID has significant effects.
- All the user information will be updated automatically to reflect the change

Related Commands

- **show snmp engineID** - Displays the Engine Identifier
- **show snmp user** - Displays the configured SNMP users

9.11 snmp proxy name

This command configures the proxy. The no form of the command removes the proxy.

snmp proxy name <ProxyName> ProxyType {Read | Write | inform | Trap} ContextEngineID <EngineId> TargetParamsIn <TargetParam> TargetOut <TargetOut> [ContextName <ProxyContextName>] [StorageType {volatile | nonvolatile}]

no snmp proxy name <ProxyName>

Syntax Description	**ProxyName**	-	The locally arbitrary, but unique identifier associated with the tProxyEntry. . This will be the INDEX used for the Proxy Table.
	ProxyType	-	Type of message that are forwarded using the translation parameters. Options are: • Read • Write • Inform • Trap
	ContextEngineID	-	Context engine identifier contained in messages that are forwarded using the translation parameters.
	TargetParamsIn	-	This object selects an entry in the snmpTargetParamsTable. The selected entry is used to determine which row of the snmpProxyTable is to be used for forwarding the received messages.
	TargetOut	-	This object selects a management target defined in the snmpTargetAddrTable (in the SNMP-TARGET-MIB). The selected target is defined by an entry in the snmpTargetAddrTable whose index value (snmpTargetAddrName) is equal to this object. . This object is only used when selection of a single target is required (that is, when forwarding an incoming read or write request).
	ContextName	-	Context name contained in messages that are forwarded using the translation parameters.
	Storage Type	-	Storage type. Options are: • volatile • nonvolatile
Mode	Global Configuration Mode		

Package Workgroup, Enterprise and Metro

Defaults Storage Type - nonvolatile

Example

```
switch(config)# snmp proxy name proxy1 ProxyType write
ContextEngineID 80.00.08.1c.04.46.53 TargetParamsIn param2
TargetOut target2  ContextName pxyctxtname StorageType
nonvolatile
```

Related Commands

`show snmp proxy` - Displays proxy details.

9.12 snmp mibproxy name

This command configures the proxy. The no form of the command removes the proxy.

snmp mibproxy name <ProxyName> ProxyType {Read | Write | inform | Trap} mibid <MibId> TargetParamsIn <TargetParam> TargetOut <TargetOut> [StorageType {volatile | nonvolatile}]

no snmp mibproxy name <ProxyMibName>

Syntax Description

ProxyName	-	The locally arbitrary, but unique identifier associated with the tProxyEntry. . This will be the INDEX used for the Proxy Table.
ProxyType	-	Type of message that are forwarded using the translation parameters. Options are: • Read • Write • Inform • Trap
mibid	-	MIB identifier.
TargetParamsIn	-	This object selects an entry in the snmpTargetParamsTable. The selected entry is used to determine which row of the snmpProxyTable to use for forwarding the received messages.
TargetOut	-	This object selects a management target defined in the snmpTargetAddrTable (in the SNMP-TARGET-MIB). The selected target is defined by an entry in the snmpTargetAddrTable whose index value (snmpTargetAddrName) is equal to this object. . This object is only used when selection of a single target is required (that is, when forwarding an incoming read or write request).
ContextName	-	Context name contained in messages that are forwarded using the translation parameters
Storage Type	-	Storage type. Options are: • volatile • nonvolatile

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Storage Type - nonvolatile

Example

```
switch(config)# snmp mibproxy name mibproxy1 ProxyType read
mibid 1 TargetParamsIn param1 TargetOut  target1
StorageType nonvolatile
```

Related Commands

`show snmp mibproxy` - Displays proxy details.

9.13 snmp view

This command configures the SNMP view. The no form of the command removes the SNMP view.

snmp view <ViewName> <OIDTree> [mask <OIDMask>] {included | excluded} [{volatile | nonvolatile}]

no snmp view <ViewName> <OIDTree>

Syntax Description	**ViewName**	-	View Name
	OIDTree	-	Object Identifier
	OIDMask | none	-	Defines views' subtrees
	included | excluded	-	Type of view
	volatile | nonvolatile	-	Type of storage
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	View Name	-	iso/restricted
	OIDTree	-	1
	OIDMask	-	None
	View type	-	included
	Storage type	-	non-volatile

Example

```
switch(config)# snmp view v2readview 1.3.6.1 mask 1.1.1.1
included nonvolatile
```

☞ To configure an SNMP view (read/write/notify), a group must have already been created using the snmp group command and SNMP group access must be configured using the snmp access command.

Related Commands

- **`snmp access`** - Configures the SNMP group access details
- **`show snmp viewtree`** - Displays the configured SNMP Tree views
- **`show snmp group access`** - Displays the configured SNMP group access details

9.14 snmp targetaddr

This command configures the SNMP target address. The no form of the command removes the configured SNMP target address.

snmp targetaddr <TargetAddressName> param <ParamName> {<IPAddress> | <IP6Address>} [timeout <Seconds(1-1500)] [retries <RetryCount(1-3)] [taglist <TagIdentifier | none>] [{volatile | nonvolatile}] [port <integer (1-65535)>]

no snmp targetaddr <TargetAddressName>

Syntax Description	**TargetAddressName**	-	Name of the Target address (host)
	param	-	SNMP parameter Name
	IPAddress/ IP6Address	-	IP/IP6 Address of the host
	timeout	-	The time the SNMP agent waits for a response from the SNMP Manager before retransmitting the Inform Request Message
	retries	-	The Maximum number of times the agent can retransmit the Inform Request Message
	taglist	-	Tag Identifier
	volatile | nonvolatile	-	Storage type
	port	-	SNMP Manager port number for sending the TRAP/INFORM messages to SNMP Manager. This value ranges between 1 and 65535.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	ParamName	-	Internet

IPAddress	-	10.0.0.10
taglist	-	snmp
volatile | nonvolatile	-	volatile
port	-	162

Example

```
switch(config)# snmp targetaddr switchmgr param switchd
10.0.0.10 taglist mytag nonvolatile
```

☞ Target param must have been configured.

Related Commands

- **`show snmp targetaddr`** - Displays the configured SNMP target Addresses
- **`snmp targetparams`** - Configures the SNMP target parameters
- **`show snmp targetparam`** - Displays the configured SNMP Target Address Params

9.15 snmp targetparams

This command configures the SNMP target parameters. The no form of the command removes the SNMP target parameters.

snmp targetparams <ParamName> user <UserName> security-model {v1 | v2c | v3 {auth | noauth | priv}} message-processing {v1 | v2c | v3} [{volatile | nonvolatile}] [filterprofile-name <profilename>] [filter-storagetype {volatile | nonvolatile}]

no snmp targetparams <ParamName>

Syntax Description	**ParamName**	-	SNMP Parameter Name
	user	-	User Name
	security-model	-	Security Model
	auth	-	Authentication - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication
	noauth	-	no-authentication
	priv	-	Specifies both authentication and privacy
	message-processing	-	Message processing model
	volatile | nonvolatile	-	Storage type
	filterprofile-name	-	Name of the filter profile to be used for the specified target address.
	filter-storagetype	-	Storage type for the filter. This can be: • volatile - Temporary storage. Details are lost once restarted. • nonvolatile - Permanent storage. Details are present even after restart.
Mode	Global Configuration Mode		

Package Workgroup, Enterprise and Metro

Defaults

ParamName	-	internet
User/Security Name	-	None
Security Model	-	v2c
Security Level	-	NoauthNoPriv
Message Processing Model	-	v2c
Storage Type	-	Non-volatile
ParamName	-	test1
User/Security Name	-	None
Security Model	-	v1
Security Level	-	NoauthNoPriv
Message Processing Model	-	v1
Storage Type	-	Non-volatile

Example

```
switch(config)# snmp targetparams param1 user user1 security-
model v3 noauth message-processing v3
```

☞ User information must have been configured prior to the configuration of SNMP target parameters

Related Commands

- **`snmp user`** - Configures the SNMP user details
- **`snmp filterprofile`** - Creates Notify filter Table
- **`show snmp targetparam`** - Displays the configured SNMP Target Address Params
- **`show snmp user`** - Displays the configured SNMP users.

9.16 snmp user

This command configures the SNMP user details. The no form of the command removes the SNMP user details.

snmp user <UserName> [auth {md5 | sha} <passwd> [priv DES <passwd>]] [{volatile | nonvolatile}] [EngineId <EngineID>]

no snmp user <UserName> [EnginId <EngineID>]

Syntax Description	**UserName**	-	Name of the User
	auth	-	Authentication Algorithm - can be Message Digest 5 or Secure Hash Algorithm
	passwd	-	Password associated with the Authentication type
	priv DES	-	Private encryption password
	volatile | nonvolatile	-	Storage type - can be either volatile or non-volatile
	EngineId	-	SNMP engine identifier
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	UserName	-	Initial
	Authentication Protocol	-	None
	Privacy Protocol	-	None
	Storage type	-	Non-volatile
	Storage type	-	Non-volatile

Example

```
switch(config)# snmp user user1
```

☞ SNMP passwords are localized using the local SNMP engine ID

Related Commands

- **`show snmp engineID`** - Displays the Engine Identifier
- **`show snmp user`** - Displays the configured SNMP users

9.17 snmp notify

This command configures the SNMP notification details. The no form of this command removes the SNMP notification details.

snmp notify <NotifyName> tag <TagName> type {Trap | Inform} [{volatile | nonvolatile}]

no snmp notify <NotifyName>

Syntax Description	**NotifyName**	-	Notification Name
	tag	-	Tag Name
	type	-	Type of Notification
	volatile | nonvolatile		Storage type of the notification details
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	Notify Name	-	iss/iss1
	Notify Tag	-	iss/iss1
	Storage type	-	volatile
Example	`switch(config)# snmp notify note1 tag tag1 type Inform`		

Related Commands

- **show snmp notif** - Displays the configured SNMP Notifications
- **show snmp targetaddr** - Displays the configured SNMP target Addresses

9.18 snmp filterprofile

This command creates Notify filter Table. The no form of the command removes the filter entry from the table.

snmp filterprofile <profile-name> <OIDTree> [mask <OIDMask>] {included | excluded} [{volatile | nonvolatile}]

no snmp filterprofile <profilename> <OIDTree>

Syntax Description	**profile-name**	-	Name of the filter profile.
	OIDTree	-	Object Identifier
	mask <OIDMask>	-	Defines a family of subtrees, in combination with the object identifier.
	included | excluded	-	Type of filter. This indicates whether the OID and mask should be included in or excluded from the fileter profile.
	volatile | nonvolatile	-	Storage type. • volatile - Temporary storage. Details are lost once restarted. • nonvolatile - Permanent storage. Details are present even after restart.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config)# snmp filterprofile filter1 1.5 mask 1.1 included nonvolatile`		

Related Commands

- **show snmp filter table** - Displays the configured SNMP filters
- **snmp targetparams** - Configures the SNMP target parameters

9.19 snmp-server enable traps snmp authentication

This command enables generation of authentication traps for SNMPv1 and SNMPv2c. The no form of the command disables generation of authentication traps for SNMPv1 and SNMPv2c.

snmp-server enable traps snmp authentication

no snmp-server enable traps snmp authentication

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	Generation of authentication traps is disabled by default.
Example	`switch(config)# snmp-server enable traps snmp authentication`

9.20 snmp-server trap udp-port

This command configures the udp port over which agent sends the trap. The no form of the command configures the snmp agent to sent trap on default udp port.

snmp-server trap udp-port <port>

no snmp-server trap udp-port

Syntax Description	**port**	-	Port number
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config)# snmp-server trap udp-port 1234`		

Related Commands

show snmp notif - Displays the configured SNMP Notification types.

9.21 snmp-server trap proxy-udp-port

This command configures the udp port over which agent sends the trap. The no form of the command configures the snmp agent to sent trap on default udp port.

snmp-server trap proxy-udp-port <port>

no snmp-server trap proxy-udp-port

Syntax Description	**port**	-	Port number
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	162		
Example	`switch(config)# snmp-server trap proxy-udp-port 162`		

Related Commands

show snmp-server proxy-udp-port - Displays the proxy udp port.

9.22 snmp agent port

This command configures the agent port on which agent listens.

snmp agent port <port>

Syntax Description	**port**	-	Port number. This value ranges between 1 and 65535.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	161		
Example	`switch(config)# snmp agent port 100`		

Related Commands

show snmp - Displays the status information of SNMP communications

9.23 snmp tcp enable

This command enables sending snmp messages over tcp. The no form of the command disables sending snmp messages over tcp.

`snmp tcp enable`

`no snmp tcp enable`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	Disabled
Example	`switch(config)# snmp tcp enable`

Related Commands

`show snmp tcp` - Displays the configuration for snmp over tcp.

9.24 snmp trap tcp enable

This command enables sending snmp trap messages over tcp. The no form of the command disables sending snmp trap messages over tcp.

`snmp trap tcp enable`

`no snmp trap tcp enable`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	Disabled
Example	`switch(config)# snmp trap tcp enable`

Related Commands

`show snmp tcp` - Displays the configuration for snmp over tcp.

9.25 snmp-server tcp-port

This command configures the tcp port over which agent sends the snmp message. The no form of the command configures the snmp agent to sent snmp message on default tcp port.

snmp-server tcp-port <port>

no snmp-server tcp-port

Syntax Description	**port**	-	Port number
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	161		
Example	`switch(config)# snmp-server tcp-port 161`		

Related Commands

show snmp tcp - Displays the configuration for snmp over tcp.

9.26 snmp-server trap tcp-port

This command configures the tcp port over which agent sends the trap. The no form of the command configures the snmp agent to sent trap on default tcp port.

snmp-server trap tcp-port <port>

no snmp-server trap tcp-port

Syntax Description	**port**	-	Port number
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	162		
Example	`switch(config)# snmp-server trap tcp-port 162`		

Related Commands

show snmp tcp - Displays the configuration for snmp over tcp.

9.27 snmp-server enable traps

This command enables generation of a particular trap. The no form of the command disables generation of a particular trap.

snmp-server enable traps {[firewall-limit] [linkup] [linkdown] [sip-states] [sip-cfg-change] [coldstart] [poe-power] [dhcp-pool-limit] [dsx1-line]}

no snmp-server enable traps {[firewall-limit] [linkup] [linkdown] [sip-states] [sip-cfg-change] [coldstart] [poe-power] [dhcp-pool-limit] [dsx1-line]}

Syntax Description	**firewall-limit**	-	Firewall attack summary trap
	linkup	-	Linkup trap
	linkdown	-	Linkdown trap
	sip-states	-	SIP states trap
	sip-cfg-change	-	SIP configuration change trap
	coldstart	-	Coldstart trap
	poe-power	-	Power on Ethernet trap
	dhcp-pool-limit	-	DHCP Server pool limit trap
	dsx1-line	-	DSX1 line trap
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config)# snmp-server enable traps firewall-limit`		

Related Commands

show snmp-server traps - Displays the set of traps that are currently enabled.

9.28 show snmp

This command displays the status information of SNMP communications.

show snmp

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
switch# show snmp

0 SNMP Packets Input
    0 Bad SNMP Version errors
    0 Unknown community name
    0 Get request PDUs
    0 Get Next PDUs
    0 Set request PDUs

0 SNMP Packets Output
    0 Too big errors
    0 No such name errors
    0 Bad value errors
    0 General errors
    0 Trap PDUs

0 SNMP Rollback failures

SNMP Manager-role output packets
    0 Drops

SNMP Informs:
    0 Inform Requests generated
    0 Inform Responses received
    0 Inform messages Dropped
    0 Inform Requests awaiting Acknowledgement

SNMP Trap Listen Port is 162
```

```
snmp agent port : 170
```

Related Command

`snmp agent port` - Configures the agent port on which agent listens

9.29 show snmp community

This command displays the configured SNMP community details.

`show snmp community`

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show snmp community`

```
Community Index: NETMAN
Community Name: NETMAN
Security Name: none
Context Name:
Transport Tag:
Storage Type: volatile
Row Status: active
------------------------------
Community Index: PUBLIC
Community Name: PUBLIC
Security Name: none
Context Name:
Transport Tag:
Storage Type: volatile
Row Status: active
```

Related Command

`snmp community index` - Configures the SNMP community details

9.30 show snmp group

This command displays the configured SNMP groups.

`show snmp group`

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro

Example	`switch# show snmp group`
	`Security Model: v1`
	`Security Name: none`
	`Group Name: iso`
	`Storage Type: volatile`
	`Row Status: active`
	`------------------------------`
	`Security Model: v2c`
	`Security Name: none`
	`Group Name: iso`
	`Storage Type: volatile`
	`Row Status: active`
	`------------------------------`

```
Security Model: v3
Security Name: initial
Group Name: initial
Storage Type: nonVolatile
Row Status: active
------------------------------
Security Model: v3
Security Name: templateMD5
Group Name: initial
Storage Type: nonVolatile
Row Status: active
------------------------------
Security Model: v3
Security Name: templateSHA
Group Name: initial
Storage Type: nonVolatile
Row Status: active
```

Related Commands

- **`snmp group`** - Configures the SNMP group details
- **`snmp user`** - Configures the SNMP user details

9.31 show snmp group access

This command displays the configured SNMP group access details.

`show snmp group access`

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show snmp group access`

```
Group Name: iso
```

```
Read View: iso
Write View: iso
Notify View: iso
Storage Type: volatile
Row Status: active
------------------------------
Group Name: iso
Read View: iso
Write View: iso
Notify View: iso
Storage Type: volatile
Row Status: active
------------------------------
Group Name: initial
Read View: restricted
Write View: restricted
Notify View: restricted
Storage Type: nonVolatile
Row Status: active
------------------------------
Group Name: initial
Read View: iso
Write View: iso
Notify View: iso
Storage Type: nonVolatile
Row Status: active
```

Related Commands

- **`snmp access`** - Configures the SNMP group access details
- **`snmp view`** - Configures the SNMP view

9.32 show snmp engineID

This command displays the Engine Identifier.

show snmp engineID

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show snmp engineID` `EngineId: 80.00.08.1c.04.46.53`

Related Command

snmp engineid - Configures the engine identifier

9.33 show snmp proxy

This command displays proxy details.

show snmp proxy

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro

Example

```
switch# show snmp proxy

Proxy Name                : PROXY1
Proxy ContextEngineID     : 80.00.08.1c.04.46.54
Proxy ContextName         :
Proxy TargetParamIn       : param1
Proxy SingleTargetOut     : Tgt1
Proxy MultipleTargetOut   :
Proxy Type                : Read
Storage Type              : Non-volatile
Row Status                : Active
-----------------------------------------------------
Proxy Name                : PROXY2
Proxy ContextEngineID     : 80.00.08.1c.04.46.54
Proxy ContextName         :
Proxy TargetParamIn       : param1
Proxy SingleTargetOut     : Tgt1
Proxy MultipleTargetOut   :
Proxy Type                : Write
Storage Type              : Non-volatile
Row Status                : Active
-----------------------------------------------------
```

Related Command

`snmp proxy name` - Configures the proxy.

9.34 show snmp mibproxy

This command displays proxy details.

show snmp mibproxy

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
switch# show snmp mibproxy
Prop Proxy Name                : proxy1
Prop MibID                     : 2
Prop Proxy TargetParamIn       : param1
Prop Proxy SingleTargetOut     : target1
Prop Proxy MultipleTargetOut   :
Prop Proxy Type                : Read
Prop Storage Type              : Non-volatile
Prop Row Status                : Active
-----------------------------------------------------
```

Related Command

snmp mibproxy name - Configures the proxy.

9.35 show snmp viewtree

This command displays the configured SNMP Tree views.

show snmp viewtree

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show snmp viewtree`

```
View Name: iso
Subtree OID: 1
Subtree Mask:
View Type: included
Storage Type: nonVolatile
Row Status: active
------------------------------
View Name: restricted
Subtree OID: 1
Subtree Mask:
View Type: included
Storage Type: nonVolatile
Row Status: active
------------------------------
```

Related Command

snmp view - Configures the SNMP view

9.36 show snmp targetaddr

This command displays the configured SNMP target Addresses.

show snmp targetaddr

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# sh snmp targetaddr`

```
Target Address Name : ht231
IP Address          : 12.0.0.100
Port                : 150
Tag List            : tg231
Parameters          : pa231
Storage Type        : Non-volatile
Row Status          : Active
------------------------------
```

Related Commands

- **snmp targetaddr** - Configures the SNMP target address
- **snmp targetparams** - Configures the SNMP target parameters
- **snmp notify** - Configures the SNMP notification details

9.37 show snmp targetparam

This command displays the configured SNMP Target Address Params.

show snmp targetparam

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
switch# sh snmp targetparam

Target Parameter Name    : internet
Message Processing Model : v2c
Security Model           : v2c
Security Name            : none
Security Level           : No Authenitcation, No Privacy
Storage Type             : Non-volatile
Row Status               : Active
Filter Profile Name      : None
Row Status               : Active
------------------------------
Target Parameter Name    : pa231
Message Processing Model : v3
Security Model           : v3
Security Name            : u231
Security Level           : No Authenitcation, No Privacy
Storage Type             : Volatile
Row Status               : Active
Filter Profile Name      : filter1
Row Status               : Active
------------------------------
Target Parameter Name    : test1
Message Processing Model : v2c
Security Model           : v1
```

```
Security Name            : none
Security Level           : No Authenitcation, No Privacy
Storage Type             : Non-volatile
Row Status               : Active
Filter Profile Name      : None
Row Status               : Active
------------------------------
```

Related Commands

- **`snmp targetparams`** - Configures the SNMP target parameters
- **`snmp user`** - Configures the SNMP user details

9.38 show snmp user

This command displays the configured SNMP users.

`show snmp user`

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show snmp user`

```
Engine ID: 80.00.08.1c.04.46.53
User: initial
Authentication Protocol: none
Privacy Protocol: none
Storage Type: nonVolatile
Row Status: active
------------------------------
Engine ID: 80.00.08.1c.04.46.53
User: templateMD5
Authentication Protocol: MD5
Privacy Protocol: none
Storage Type: nonVolatile
```

```
Row Status: active
------------------------------
Engine ID: 80.00.08.1c.04.46.53
User: templateSHA
Authentication Protocol: SHA
Privacy Protocol: DES_CBC
Storage Type: nonVolatile
Row Status: active
------------------------------
```

Related Commands

- **`snmp user`** - Configures the SNMP user details
- **`show snmp community`** - Displays the configured SNMP community details

9.39 show snmp notif

This command displays the configured SNMP Notification types.

`show snmp notif`

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro

Example

```
switch# show snmp notif
Notify Name: iss
Notify Tag: iss
Notify Type: trap
Storage Type: volatile
Row Status: active
------------------------------
Notify Name: iss1
Notify Tag: iss1
Notify Type: trap
Storage Type: volatile
Row Status: active
```

Related Commands

- **`snmp notify`** - Configures the SNMP notification details
- **`snmp targetparams`** - Configures the SNMP target parameters

9.40 show snmp inform statistics

This command displays the inform message statistics.

`show snmp inform statistics`

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro

Example

```
switch# show snmp inform statistics

Target Address Name  : issmanager
IP Address           : 10.0.0.10
Inform messages sent : 20
Acknowledgement awaited for : 2 Inform messages
Inform messages dropped : 0
Acknowledgement failed for : 0 Inform messages
Informs retransmitted: 0
Inform responses received: 18
```

☞ SNMP Manager must have been configured and Inform type notifications must have been generated.

9.41 Show snmp-server traps

This command displays the set of traps that are currently enabled.

`show snmp-server traps`

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
switch# show snmp-server traps

Currently enabled traps:
------------------------
linkup,linkdown,
```

Related Command

`snmp-server enable traps` - Enables generation of a particular trap.

9.42 show snmp-server proxy-udp-port

This command displays the proxy udp port.

show snmp-server proxy-udp-port

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show snmp-server proxy-udp-port` `snmp-server proxy-udp-port : 162`

Related Command

snmp-server trap proxy-udp-port - Configures the udp port over which agent sends the trap.

9.43 show snmp tcp

This command displays the configuration for snmp over tcp.

show snmp tcp

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	switch# show snmp tcp snmp over tcp disabled snmp trap over tcp disabled snmp listen tcp port 161 Snmp listen tcp trap port 162

Related Command

- **snmp tcp enable** – Enables sending snmp messages over tcp.
- **snmp trap tcp enable** - Enables sending snmp trap messages over tcp.
- **snmp-server tcp-port** – Configures the tcp port over which agent sends the snmp message.
- **snmp-server trap tcp-port** - Configures the tcp port over which agent sends the trap.

9.44 show snmp filter table

This command displays the configured SNMP filters.

show snmp filter table

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro

Example	`switch# show snmp filter table`
	`Filter Name  : filter1`
	`Subtree OID  : 1.5`
	`Subtree Mask : 1.1`
	`Filter Type  : Included`
	`Storage Type : Non-volatile`
	`Row Status   : Active`
	`------------------------------`

Related Command

- **snmp filterprofile** - Creates Notify filter Table

Chapter 10

10.SNTP

The SNTP (Simple Network Time Protocol) module is used to synchronize the time and date in ISS by contacting the SNTP Server. It supports different time zones, where the user can set the required time zone.

The following are the list of SNTP commands:

- sntp
- set sntp client
- set sntp client version
- set sntp client addressing mode
- set sntp client port
- set sntp client clock-format
- set sntp time zone
- set sntp client clock-summer-time
- set sntp client authentication-key
- set sntp unicast-server auto-discovery
- set sntp unicast-poll-interval
- set sntp unicast-max-poll-timeout
- set sntp unicast-max-poll-retry
- set sntp unicast-server
- set sntp broadcast-mode send-request
- set sntp broadcast-poll-timeout
- set sntp broadcast-delay-time
- set sntp multicast-mode send-request

- set sntp multicast-poll-timeout
- set sntp multicast-delay-time
- set sntp multicast-group-address
- set sntp anycast-poll-interval
- set sntp anycast-poll-timeout
- set sntp anycast-poll-retry-count
- set sntp anycast-server
- set sntp client clock-format
- show sntp status
- show sntp unicast–mode status
- show sntp broadcast–mode status
- show sntp multicast–mode status
- show sntp anycast–mode status
- debug sntp

10.1 sntp

This command enters SNTP configuration mode.

`sntp`

Mode	Profile configuration mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# sntp` `switch(config-sntp)#`

10.2 set sntp client

This command enables or disables SNTP client module.

`set sntp client {enabled | disabled}`

Syntax Description	**`enabled`**	-	Enables the SNTP client module
	`disabled`	-	Disables the SNTP client module
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	disabled		
Example	`switch(config-sntp)# set sntp client enabled`		
☞	SNTP client should be enabled		

Related Command

- **`show sntp status`**: Displays SNTP status

10.3 set sntp client version

This command sets the operating version of the SNTP for the client.

`set sntp client version { v1 | v2 | v3 | v4 }`

Syntax Description	**v1**	-	SNTP Version 1
	v2	-	SNTP Version 2
	v3	-	SNTP Version 3
	v4	-	SNTP Version 4
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	v4		
Example	`switch(config-sntp)# set sntp client version v3`		
☞	SNTP client should be enabled		

Related Command

- **`show sntp status`**: Displays SNTP status

10.4 set sntp client addressing mode

This command sets the addressing mode of SNTP client as either unicast, multicast, broadcast, anycast.

`set sntp client addressing-mode { unicast | broadcast | multicast | anycast }`

Syntax Description	**`unicast`**	-	Sets the addressing mode of SNTP client as unicast.
	`broadcast`	-	Sets the addressing mode of SNTP client as broadcast.
	`multicast`		Sets the addressing mode of SNTP client as multicast
	`anycast`	-	Sets the addressing mode of SNTP client as anycast.

Mode	SNTP Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	unicast
Example	`switch(config-sntp)# set sntp client addressing-mode unicast`
☞	SNTP client should be enabled

Related Command

- **`show sntp anycast-mode status –`** Displays the SNTP anycast mode status
- **`show sntp broadcast-mode status –`** Displays the SNTP broadcast mode status
- **`show sntp multicast-mode status`** – Displays the SNTP multicast mode status
- **`show sntp status`**: Displays SNTP status
- **`show sntp unicast-mode status`** - Displays the SNTP Unicast Mode status

10.5 set sntp client port

This command sets the listening port for SNTP client greater than 1024 as below 1024 are reserved. Therefore the configurable listening port for SNTP client starts at 1025.The no form of command deletes the listening port for SNTP client and sets the default value.

set sntp client port <portno(1025-65535)>

no sntp client port

Syntax Description	**port no**	-	Listening port for SNTP client
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	123		
Example	`switch (config-sntp)# set sntp client port 1026`		
☞	SNTP client should be enabled		

Related commands

- **show sntp status**: Displays SNTP status

10.6 set sntp client clock-format

This command sets the system clock format as AM PM format or HOURS format.

`set sntp client clock-format {ampm | hours}`

Syntax Description	**`am-pm`**	-	Sets the system clock in am/ pm format
	`hours`	-	Sets the system clock in 24 hours format
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Default	hours		
Example	`switch (config-sntp)# set sntp client clock-format ampm`		
☞	SNTP clock format configuration in the Switch: • Date – Hours, Minutes, Seconds, Date Month and Year • Month – Jan, Feb, Mar….. • Year - yyyy		

Related Command

- **`show sntp clock`** - Displays the current time.

10.7 set sntp time zone

This command sets the system time zone with respect to UTC. The no form of command resets the system time zone to GMT.

set sntp client time-zone <+/- UTC TimeDiff in Hrs:UTC TimeDiff in Min> Eg: +05:30

no sntp client time-zone

Syntax Description	**+/-**	-	After or before UTC
	UTCTimeDiff in Hrs	-	UTC Time difference in hours
	UTC TimeDiff in Min	-	UTC Time difference in minutes
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config-sntp)# set sntp client time-zone +05:30`		
☞	SNTP server must be enabled prior to the execution of this command.		

Related Command

- **show sntp status**: Displays SNTP status

10.8 set sntp client clock-summer-time

This command enables the Daylight Saving Time. The no form of the command disables the Daylight Saving Time.

set sntp client clock-summer-time <week-day-month,hh:mm> <week-day-month,hh:mm> Eg: set sntp client clock-summer-time First-Sun-Mar,05:10 Second-Sun-Nov,06:10

no sntp client clock summer-time

Syntax Description	**week-day-month**	-	Week – First, Second, Third, Fourth or Last week of month. Day –Sunday, Monday, Tuesday, Wednesday, Thursday, Friday or Saturday. Month: January, February, March, April, May, June, July, August, September, October, November or December.
	hh:mm	-	Time in hours and minutes
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config-sntp)# set sntp client clock-summer-time First-Sun-Jan,12:12 Second-Sun-Mar,12:12`		

Related Commands:

- **show sntp status**: Displays SNTP status

10.9 set sntp client authentication-key

This command sets the authentication parameters. The no form of the command disables authentication.

set sntp client authentication-key <key-id> md5 <key>

no sntp client authentication

Syntax Description	**key-id**	-	Key Identifier (integer value). Range is 1 – 65535.
	md5	-	Message Digest Algorithm
	key	-	Key value (string value)
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config-sntp)# set sntp client authentication-key 123 md5 Garland Technology`		
☞	SNTP client should be enabled		

Related Command

- **show sntp status**: Displays SNTP status

10.10 set sntp unicast-server auto-discovery

This command configures SNTP client status of auto-discovery of server.

`set sntp unicast-server auto-discovery {enabled | disabled}`

Syntax Description	**`enabled`**	-	Enables the auto discovery of server
	`disabled`	-	Disables the auto discovery of server
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	disabled		
Example	`switch(config-sntp)# set sntp unicast-server auto-discovery enabled`		
☞	SNTP client addressing mode should be unicast		

Related Command

- **`show sntp unicast–mode status`** - Displays the SNTP Unicast Mode status

10.11 set sntp unicast-poll-interval

This command configures SNTP client poll interval.

`set sntp unicast-poll-interval <value (16-16284) seconds>`

Syntax Description	**`value`**	-	Poll interval value in seconds.
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Default	64		
Example	`switch(config-sntp)# set sntp unicast-poll-interval 50`		
☞	SNTP client addressing mode should be unicast		

Related Command

- **`show sntp unicast–mode status`** - Displays the SNTP Unicast Mode status

10.12 set sntp unicast-max-poll-timeout

This command configures SNTP client maximum poll interval timeout.

`set sntp unicast-max-poll-timeout <value (1-30) seconds>`

Syntax Description	**`value`**	-	Maximum poll interval time out value in seconds.
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Default	5		
Example	`switch(config-sntp)# set sntp unicast-max-poll-timeout 25`		
☞	SNTP client addressing mode should be unicast		

Related Command

- **`show sntp unicast–mode status`** - Displays the SNTP Unicast Mode status

10.13 set sntp unicast-max-poll-retry

This command configures SNTP client maximum retry poll count.

set sntp unicast-max-poll-retry <value (1-10) times>

Syntax Description	**value**	-	Maximum retry poll count value
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Default	3		
Example	`switch(config-sntp)# set sntp unicast-max-poll-retry 10`		
☞	SNTP client addressing mode should be unicast		

Related Command

- **show sntp unicast–mode status** - Displays the SNTP Unicast Mode status

10.14 set sntp unicast-server

This command configures SNTP unicast server attributes. The no form of command deletes the sntp unicast server attributes and sets to default.

set sntp unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr>} [{primary | Secondary}] [{version3 | version 4}] [<portid(1025-36564)>]

no sntp unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr>}

Syntax Description	**ipv4, ipv6**	-	Version 4 and Version 6 IP address
	Primary/ secondary	-	Primary/ Secondary NTP servers
	Port-id	-	Port identifier
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config-sntp)# set sntp unicast-server ipv4 12.0.0.100 Primary 3 1234`		
☞	SNTP client addressing mode should be unicast		

Related Command

- **show sntp unicast–mode status** - Displays the SNTP Unicast Mode status

10.15 set sntp broadcast-mode send-request

This command sets the status of sending the request for knowing the delay.

`set sntp broadcast-mode send-request {enabled | disabled}`

Syntax Description	**`enabled`**	-	When enabled the SNTP request packet is sent to broadcast server to calculate the actual delay.
	`disabled`	-	When disabled no SNTP request packet is sent out to broadcast server instead default value for the delay is taken.
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	disabled		
Example	`switch(config-sntp)# set sntp broadcast-mode send-request enabled`		
☞	SNTP client addressing mode should be broadcast		

Related Command

- **`show sntp broadcast–mode status –`** Displays the SNTP broadcast mode status

10.16 set sntp broadcast-poll-timeout

This command configures SNTP client poll interval in broadcast mode.

`set sntp broadcast-poll-timeout [<value (1-30) seconds>]`

Syntax Description	**`value`**	-	Poll interval time out value in seconds for broadcast mode
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Default	5		
Example	`switch(config-sntp)# set sntp broadcast-poll-timeout 30`		
☞	SNTP client addressing mode should be broadcast		

Related Command

- **`show sntp broadcast–mode status –`** Displays the SNTP broadcast mode status

10.17 set sntp broadcast-delay-time

This command configures SNTP delay time in broadcast mode.

`set sntp broadcast-delay-time [<value (1000-15000) microseconds>]`

Syntax Description	**`value`**	-	Delay time value in micro seconds in broadcast mode
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Default	8000		
Example	`switch(config-sntp)# set sntp broadcast-delay-time 2000`		
☞	SNTP client addressing mode should be broadcast		

Related Command

- **`show sntp broadcast–mode status –`** Displays the SNTP broadcast mode status

10.18 set sntp multicast-mode send-request

This command sets the status of sending the request for knowing the delay.

`set sntp multicast-mode send-request {enabled | disabled}`

Syntax Description	**`enabled`**	-	When enabled the SNTP request packet is sent to broadcast server to calculate the actual delay.
	`disabled`	-	When disabled no SNTP request packet is sent out to broadcast server instead default value for the delay is taken.
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	disabled		
Example	`switch(config-sntp)# set sntp multicast-mode send-request enabled`		
☞	SNTP client addressing mode should be multicast		

Related Command

- **`show sntp multicast–mode status`** – Displays the SNTP multicast mode status

10.19 set sntp multicast-poll-timeout

This command configures SNTP client poll interval in multicast mode.

`set sntp multicast-poll-timeout [<value (1-30) seconds>]`

Syntax Description	**`value`**	-	Poll interval time out value in seconds in multicast mode
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Default	5		
Example			

```
switch(config-sntp# set sntp multicast-poll-timeout 10
```

☞ SNTP client addressing mode should be multicast

Related Command

- **`show sntp multicast-mode status`** – Displays the SNTP multicast mode status

10.20 set sntp multicast-delay-time

This command configures SNTP delay time in multicast mode.

set sntp multicast-delay-time [<value (1000-15000) microseconds>]

Syntax Description	**value**	-	Delay time value in micros seconds in multicast mode
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Default	8000		
Example	`switch(config-sntp)# set sntp multicast-delay-time 2000`		
☞	SNTP client addressing mode should be multicast		

Related Command

- **show sntp multicast–mode status** – Displays the SNTP multicast mode status

10.21 set sntp multicast-group-address

This command configures SNTP multicast group address.

set sntp multicast-group-address {ipv4 {<mcast_addr> | default} | ipv6 {<ipv6_addr> | default}}

Syntax Description	**ipv4, ipv6**	-	Version4, Version 6 multicast group address
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config-sntp)# set sntp multicast-group-address ipv4 224.1.1.10.`		
☞	SNTP client addressing mode should be multicast		

Related Command

- **show sntp multicast–mode status** – Displays the SNTP multicast mode status

10.22 set sntp anycast-poll-interval

This command configures SNTP client poll interval in anycast mode.

`set sntp anycast-poll-interval [<value (16-16284) seconds>]`

Syntax Description	**`value`**	-	Poll interval value in seconds in anycast mode.
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Default	64		
Example	`switch(config-sntp)# set sntp anycast-poll-interval 20`		
☞	SNTP client addressing mode should be anycast		

Related Command

- **`show sntp anycast–mode status –`** Displays the SNTP anycast mode status

10.23 set sntp anycast-poll-timeout

This command configures SNTP client poll timeout in anycast mode.

set sntp anycast-poll-timeout [<value (1-30) seconds>]

Syntax Description	**value**	-	Poll interval time out value in seconds in anycast mode
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Default	5		
Example	`switch(config-sntp)# set sntp anycast-poll-timeout 10`		
☞	SNTP client addressing mode should be anycast		

Related Command

- **show sntp anycast–mode status –** Displays the SNTP anycast mode status

10.24 set sntp anycast-poll-retry-count

This command configures SNTP poll retries in anycast mode.

set sntp anycast-poll-retry-count [<value (1-10)>]

Syntax Description	**value**	-	Maximum retry poll count value in anycast mode
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Default	3		
Example	`switch(config-sntp)# set sntp anycast-poll-retry-count 5`		
☞	SNTP client addressing mode should be anycast		

Related Command

- **show sntp anycast–mode status –** Displays the SNTP anycast mode status

10.25 set sntp anycast-server

This command configures SNTP multicast or broadcast server address in anycast mode.

set sntp anycast-server { broadcast | multicast {ipv4 [<ipv4_addr>] |ipv6 [<ip6_addr>]} }

Syntax Description	**broadcast**	-	Configures SNTP broadcast server address in anycast mode
	multicast	-	Configures SNTP multicast server address in anycast mode.
	ipv4,ipv6	-	Version 4, Version 6
	ipv4 addr, ip6 addr	-	Version 4/ Version 6 any cast address
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config-sntp)# set sntp anycast-server ipv4 12.0.0.100`		

☞ SNTP client addressing mode should be anycast

Related Command

- **show sntp anycast–mode status –** Displays the SNTP anycast mode status

10.26 show sntp clock

This command displays the current time.

show sntp clock

Mode	User EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	switch# show sntp clock current time : Sat Jan 01 2000 00:07:04 (UTC + 0: 0)

Related Command

- Displays the system date and time.

10.27 show sntp status

This command displays SNTP status.

show sntp status

Mode	User EXEC Mode
Package	Workgroup, Enterprise and Metro

Example

```
switch# show sntp status

sntp client is enabled
current sntp client version is v4
current sntp client addressing mode is unicast
sntp client port is 123
sntp client clock format is 24 hours
sntp client authenticatin key id is 5
sntp client authentication algorithm is md5
sntp client auth Key is Garland Technology
sntp client time zone is  + 05:30
sntp client dst start time is not set
sntp client dst end time is not set
```

Related Command

- **show sntp unicast–mode status** – Displays the SNTP Unicast Mode status
- **show sntp broadcast–mode status** – Displays the SNTP broadcast mode status
- **show sntp multicast–mode status** - Displays the SNTP multicast mode status
- **show sntp anycast–mode status** - Displays the SNTP anycast mode status

10.28 show sntp unicast–mode status

This command displays the SNTP Unicast Mode status.

show sntp unicast-mode status

Mode — User EXEC Mode

Package — Workgroup, Enterprise and Metro

Example

```
switch# show sntp unicast-mode status

auto discovery of sntp/ntp servers is disabled
unicast poll interval value is 50
unicast max poll time out value is 25
unicast max retry time value is 10
unicast primary server address is 12.0.0.100
unicast primary server version is 3
unicast primary server port is 1234
```

Related Command

- **set sntp unicast-server auto-discovery** - Configures SNTP client status of auto-discovery of server
- **set sntp unicast-poll-interval** - Configures SNTP client poll interval
- **set sntp unicast-max-poll-timeout** - Configures SNTP client maximum poll interval timeout
- **set sntp unicast-max-poll-retry** - Configures SNTP client maximum retry poll count

10.29 show sntp broadcast–mode status

This command displays the SNTP broadcast mode status.

show sntp broadcast-mode status

Mode User EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
switch# show sntp broadcast-mode status

send sntp request to server in broadcast mode is disabled
broadcast poll time out value is 5
broadcast delay time value is 8000
broadcast sntp server is 12.0.0.100
```

Related Command

- **`set sntp broadcast-mode send-request`** - Sets the status of sending the request for knowing the delay
- **`set sntp broadcast-poll-timeout`** - Configures SNTP client poll interval in broadcast mode
- **`set sntp broadcast-delay-time`** - Configures SNTP delay time in broadcast mode

10.30 show sntp multicast–mode status

This command displays the SNTP multicast mode status.

`show sntp multicast-mode status`

Mode	User EXEC Mode
Package	Workgroup, Enterprise and Metro

Example	`switch# show sntp multicast-mode status`
	`send sntp request to server in multicast mode is disabled`
	`multicast poll time out value is 5`
	`multicast delay time value is 8000`
	`multicast group address is 12.0.0.100`

Related Command

- **`set sntp multicast-mode send-request` -** Sets the status of sending the request for knowing the delay
- **`set sntp multicast-poll-timeout` -** Configures SNTP client poll interval in multicast mode
- **`set sntp multicast-delay-time` -** Configures SNTP delay time in multicast mode
- **`set sntp multicast-group-address` -** Configures SNTP multicast server address

10.31 show sntp anycast–mode status

This command displays the SNTP anycast mode status.

show sntp anycast-mode status

Mode	User EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	switch# show sntp anycast-mode status anycast poll interval value is 64 anycast max poll time out value is 5 anycast max retry time value is 3 anycast server type is broadcast primary server address is 12.0.0.100

Related Command

- **set sntp anycast-poll-interval -** Configures SNTP client poll interval in anycast mode
- **set sntp anycast-poll-timeout -** Configures SNTP client poll timeout in anycast mode
- **set sntp anycast-poll-retry-count -** Configures SNTP poll retries in anycast mode

10.32 debug sntp

This command enables SNTP trace. The no form of the command disables the SNTP trace.

debug sntp {all | [init-shut] [mgmt] [data-path] [control] [pkt-dump] [resource] [all-fail] [buff]}

no debug sntp {all | [init-shut] [mgmt] [data-path] [control] [pkt-dump] [resource] [all-fail] [buff]}

Syntax Description	**init/shut**	-	Initialization/ Shutdown messages
	mgmt	-	Management Messages
	data-path	-	Data Path Messages
	control	-	Control Messages
	pkt-dump	-	Packet Dump Messages
	resource	-	Resource Messages
	all-fail	-	All failure Messages
	buff	-	Buffer Message
Mode	User EXEC Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	Debugging is Disabled		
Example	`debug sntp all`		

Chapter 11

11.RMON

RMON (Remote Monitoring) is a standard monitoring specification5 that enables various network monitors and console systems to exchange network-monitoring data.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

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

- set rmon
- rmon collection history
- rmon collection stats
- rmon event
- rmon alarm
- show rmon

11.1 set rmon

This command is used to enable or disable the RMON feature.

`set rmon {enable | disable}`

Syntax Description	**`enable`**	-	Enables the RMON feature in the system
	`disable`	-	Disables the RMON feature in the system
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	The RMON Module is disabled by default		
Example	`switch(config)# set rmon enable`		

☞ All the other RMON Module commands can be executed only when the RMON Module is enabled. Fatal error messages are displayed when commands are executed without enabling the RMON feature.

Related Command

`show rmon` - Successful execution of this command without any messages indicates that RMON feature is enabled in the system

11.2 rmon collection history

This command enables history collection of interface statistics in the buckets for the specified time interval. The no form of the command disables the history collection on the interface.

rmon collection history <index (1-65535)> [buckets <bucket-number (1-65535)>] [interval <seconds (1-3600)>] [owner <ownername (127)>]

no rmon collection history <index (1-65535)>

Syntax Description	**index**	-	History table index
	buckets	-	The maximum number of buckets desired for the RMON collection history group of statistics
	interval	-	The number of seconds in each polling cycle
	owner	-	Optional field - allows the user to enter the name of the owner of the RMON group of statistics
Mode	Interface Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	bucket number	-	50
	interval	-	1800 seconds
	owner	-	monitor

Example

```
switch(config-if)# rmon collection history 1 buckets 2 interval
20
```

- The RMON feature must be enabled for the successful execution of this command.
- The polling cycle is the bucket interval where the interface statistics details are stored.

Related Command

show rmon - Displays the history collection for the configured bucket (show rmon history [history-index (1-65535)>])

11.3 rmon collection stats

This command enables RMON statistic collection on the interface. The no form of the command disables RMON statistic collection on the interface.

rmon collection stats <index (1-65535)> [owner <ownername (127)>]

no rmon collection stats <index (1-65535)>

Syntax Description	**index**	-	Statistics table index
	owner	-	Optional field - allows the user to enter the name of the owner of the RMON group of statistics with a string length of 127
Mode	Interface Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	owner	-	monitor
Example	`switch(config-if)# rmon collection stats 1`		

☞ The RMON feature must be enabled for the successful execution of this command.

Related Command

show rmon - Displays the RMON collection statistics (show rmon statistics [<stats-index (1-65535)>])

11.4 rmon event

This command adds an event to the RMON event table. The added event is associated with an RMON event number. The no form of the command deletes an event from the RMON event table.

rmon event <number (1-65535)> [description <event-description (127)>] [log] [owner <ownername (127)>] [trap <community (127)>]

no rmon event <number (1-65535)>

Syntax Description	**number**	-	Event number
	description	-	Description of the event
	log	-	Used to generate a log entry
	owner	-	Owner of the event
	trap	-	Used to generate a trap. The SNMP community string is to be passed for the specified trap.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	`switch(config)# rmon event 1 log owner Garland Technology trap NETMAN`		

☞ The RMON feature must be enabled for the successful execution of this command.

Related Commands

- **rmon alarm** - Sets an alarm on a MIB object
- **show rmon events** - Displays the RMON events
- **show rmon alarms** - Displays the RMON alarms
- **show snmp community** - Configures the SNMP community details

11.5 rmon alarm

This command sets an alarm on a MIB object. The Alarm group periodically takes statistical samples from variables in the probe and compares them to thresholds that have been configured. The no form of the command deletes the alarm configured on the MIB object.

rmon alarm <alarm-number> <mib-object-id (255)> <sample-interval-time (1-65535)> {absolute | delta} rising-threshold <value (0-2147483647)> [rising-event-number (1-65535)] falling-threshold <value (0-2147483647)> [falling-event-number (1-65535)] [owner <ownername (127)>]

no rmon alarm <number (1-65535)>

Syntax Description	**alarm-number**	-	Alarm Number. This value ranges between 1 and 65535.
	mib-object-id	-	The mib object identifier
	sample-interval-time	-	Time in seconds during which the alarm monitors the MIB variable. This value ranges between 1 and 65535 seconds.
	absolute	-	Used to test each mib variable directly
	delta		Used to test the change between samples of a variable
	rising-threshold	-	A number at which the alarm is triggered. This value ranges between 0 and 2147483647.
	falling-threshold value	-	A number at which the alarm is reset. This value ranges between 0 and 2147483647.
	rising-event-number	-	The event number to trigger when the rising threshold exceeds its limit. This value ranges between 1 and 65535. . This feature is optional only in the code using the industrial standard command, otherwise this feature is mandatory.
	falling-event-number	-	The event number to trigger when the falling threshold exceeds its limit. This value ranges between 1 and 65535. . This feature is optional only in the code using the industrial standard command, otherwise this feature is mandatory.
	owner	-	Owner of the alarm
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		

Defaults By default, the least event number in the event table is assigned for the rising and falling threshold as its event number.

Example

```
switch(config)# rmon alarm 4
1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 2 absolute rising-
threshold 2 2 falling-threshold 1 2 owner Garland Technology
```

☞

- The RMON Feature must be enabled for the successful execution of this command
- RMON events must have been configured
- In the **Garland Technology FAB Switch**, we cannot monitor all the mib objects through RMON. This will be applicable only to the Ethernet interfaces
- Falling threshold should be less than rising threshold.

Related Commands

- **`rmon collection stats`** - Enables RMON statistic collection on the interface
- **`rmon event`** - Adds an event to the RMON event table
- **`show rmon alarms`** - Displays the RMON alarms
- **`show rmon events`** - Displays the RMON events

11.6 show rmon

This command displays the RMON statistics, alarms, events, and history configured on the interface.

show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [history [history-index (1-65535)] [overview]]

Syntax Description	**statistics**	-	The configured stats index value
	alarms	-	The configured alarm
	events	-	The configured event
	history	-	The configured history index
	overview	-	Displays only the overview of rmon history entries
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		

Example

```
switch# show rmon  statistics 2
RMON is enabled
Collection 2 on Gi0/2 is active, and owned by fsoft,
 Monitors ifEntry.1.2 which has
 Received 1240 octets, 10 packets,
 2 broadcast and 10 multicast packets,
 0 undersized and 1 oversized packets,
 0 fragments and 0 jabbers,
 0 CRC alignment errors and 0 collisions.
 # of packets received of length (in octets):
 64: 0, 65-127: 10, 128-255: 0,
 256-511: 0, 512-1023: 0, 1024-1518: 0
```

```
switch# show rmon

RMON is enabled

switch# show rmon history

RMON is enabled
Entry 1 is active,  and owned by fsoft
 Monitors ifEntry.1.1 every 3000 second(s)
 Requested # of time intervals, ie buckets, is 3,
 Granted # of time intervals, ie buckets, is 3,
  Sample 1 began measuring at 0
   Received 0 octets, 0 packets,
   0 broadcast and 0 multicast packets,
   0 undersized and 0 oversized packets,
   0 fragments and 0 jabbers,
   0 CRC alignment errors and 0 collisions,
   # of dropped packet events is 0
   Network utilization is estimated at 0
  Sample 2 began measuring at 0
   Received 0 octets, 0 packets,
   0 broadcast and 0 multicast packets,
   0 undersized and 0 oversized packets,
   0 fragments and 0 jabbers,
   0 CRC alignment errors and 0 collisions,
   # of dropped packet events is 0
   Network utilization is estimated at 0

switch# show rmon events

RMON is enabled

Event 1 is active, owned by
 Description is
 Event firing causes nothing,
 Time last sent is Aug 27 18:30:01 2009
```

```
Event 2 is active, owned by
 Description is
 Event firing causes nothing,
 Time last sent is Aug 27 18:31:36 2009
```

```
switch# show rmon alarms

RMON is enabled
Alarm 4 is active,  owned by Garland Technology
 Monitors 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 every 2
second(s)
 Taking absolute samples, last value was 3
 Rising threshold is 2, assigned to event 2
 Falling threshold is 1, assigned to event 2
 On startup enable rising or falling alarm
```

```
switch# show rmon statistics 2 alarms events  history 1

RMON is enabled
Collection 2 on Ex0/1 is active, and owned by monitor,
 Monitors ifEntry.1.1 which has
 Received 5194 octets, 53 packets,
 0 broadcast and 0 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers,
 53 CRC alignment errors and 0 collisions.
 # of packets received of length (in octets):
 64: 0, 65-127: 53, 128-255: 0,
 256-511: 0, 512-1023: 0, 1024-1518: 0
Alarm 4 is active,  owned by Garland Technology
 Monitors 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 every 2
second(s)
 Taking absolute samples, last value was 3
 Rising threshold is 2, assigned to event 2
 Falling threshold is 1, assigned to event 2
 On startup enable rising or falling alarm
```

```
Event 1 is active, owned by
 Description is
 Event firing causes nothing,
 Time last sent is Aug 27 18:30:01 2009

Event 2 is active, owned by
 Description is
 Event firing causes nothing,
 Time last sent is Aug 27 18:31:36 2009
```

```
switch# show rmon history overview
RMON is enabled
Entry 1 is active,  and owned by fsoft
 Monitors ifEntry.1.1 every 3000 second(s)
 Requested # of time intervals, ie buckets, is 3,
 Granted # of time intervals, ie buckets, is 3
```

☞ If the **show rmon** command is executed with out enabling the RMON feature, then the following output is displayed

```
switch# show rmon
RMON feature is disabled
```

Related Commands

- **set rmon** - Enables or disables the RMON feature
- **rmon collection history** - Enables history collection of interface statistics in the buckets for the specified time interval
- **rmon collection stats** - Enables RMON statistic collection on the interface
- **rmon event** - Adds an event to the RMON event table
- **rmon alarm** - Sets an alarm on a MIB object

Chapter 12

12. 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.

12.1 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.

12.2 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.

```
IM(config)# configuration map
Creating New Configuration Map :: 1
IM(config-map-1)# input-ports extreme-ethernet 0/1-5 output-ports
extreme-ethernet  0/24
```

12.3 Port Channel

Many physical ports can be grouped to form port channel. It can contain maximum 8 physical ports.

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:

Assings 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
```

12.4 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:

Assings 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
```

12.5 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)>]
```

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

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 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.

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
```

12.6 set backward-compatibility

Enables/disables backward compatibility mode. When this mode is enabled, CLI commands from older firmware will work (such as VLANs). This mode should only be enabled for debugging purposes.

set backward-compatibility { enable | disable }

Syntax Description	**enable – enables backward compatibility mode**
	disable – disables backward compatibility mode
Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# set backward-compatibility disable`

12.7 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
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# set telnet disable`

12.8 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 maps' 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
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# swap-priority cfg-map1 1 cfg-map2 2`

12.9 set parse-ip-header

This option allows the parsing of the passenger traffic for MPLS packets. This is useful for load balancing MPLS traffic based on the passenger traffic..

set parse-ip-header { enable | disable }

Syntax Description	**enable – enables parsing of IP header**
	disable – disables parsing of IP header
Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# set parse-ip-header disable`

12.10 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
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# set filter-match poll-time-interval 500`

12.11 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
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# set tagging-mode double`

12.12 shutdown cut-through

Disables cut-through mode globally.

shutdown cut-through

Syntax Description	**n/a**
Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# shutdown cut-through`

12.13 no shutdown cut-through

Enables cut-through mode globally.

no shutdown cut-through

Syntax Description	**n/a**
Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# no shutdown cut-through`

12.14 cut-through packet-length

Specifies the packet length threshold before cut-through mode will be used. For example, if the packet-length is set to “1500” and a packet with size of 1512 enters the switch, cut-through mode will be applied to this packet. If a 1400 byte packet enters the same switch, cut-through mode will not be applied. It is recommended to leave cut-through mode disabled.

cut-through packet-length <integer(150-9216)>

Syntax Description	**integer(150-9216) – Specifies the cut-through threshold**
Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# cut-through packet-length 1500`

12.15 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
Package	Workgroup, Enterprise and Metro
Example	`switch(config)# set hash-mode crc6`

12.16 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
Package	Workgroup, Enterprise and Metro
Example	`switch(config-if)# set l2-vpn-mpls-strip disable`

12.17 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
Package	Workgroup, Enterprise and Metro
Example	`switch(config-if)# set name “P1”`

12.18 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
Package	Workgroup, Enterprise and Metro
Example	`switch(config-if)# set description “Niagara 2818 input”`

12.19 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
Package	Workgroup, Enterprise and Metro
Example	`switch(config-if)# set nested-vlan disable`

12.20 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
Package	Workgroup, Enterprise and Metro
Example	`switch(config-if)# set in-traffic block`

12.21 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
Package	Workgroup, Enterprise and Metro
Example	`switch(config-if)# set out-traffic block`

12.22 set cut-through

Enables or disables cut-through mode for a specific interface.

set cut-through { enable | disable }

Syntax Description	**enable – enables cut-through mode**
	disable - disables cut-through mode
Mode	Interface Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config-if)# set cut-through enable`

12.23 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
Package	Workgroup, Enterprise and Metro
Example	`switch(config-if)# set crc-hash-policy src-ip-byte0 src-l4-port`

12.24 set force-link-up

Enables or disables force link up 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 packetmaster. This mode forces the link up so that egress traffic will continue to flow from the specific port.

`set force-link-up { enable | disable }`

Syntax Description	**`enable – enables force link up mode`**
	`disable - disables force link up mode`

Mode	Interface Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	`switch(config-if)# set force-link-up enable`

12.25 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
Package	Workgroup, Enterprise and Metro
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
Ex0/9        Disabled
Ex0/10       Disabled
Ex0/11       Disabled
Ex0/12       Disabled
Ex0/13       Disabled
Ex0/14       Disabled
Ex0/15       Disabled
Ex0/16       Disabled
Ex0/17       Disabled
Ex0/18       Disabled
Ex0/19       Disabled
```

```
Ex0/20      Disabled
Ex0/21      Disabled
Ex0/22      Disabled
Ex0/23      Disabled
Ex0/24      Disabled
Ex0/25      Disabled
Ex0/26      Disabled
Ex0/27      Disabled
Ex0/28      Disabled
Ex0/29      Disabled
Ex0/30      Disabled
Ex0/31      Disabled
Ex0/32      Disabled
Ex0/33      Disabled
Ex0/34      Disabled
Ex0/35      Disabled
Ex0/36      Disabled
Ex0/37      Disabled
Ex0/38      Disabled
Ex0/39      Disabled
Ex0/40      Disabled
Ex0/41      Disabled
Ex0/42      Disabled
Ex0/43      Disabled
Ex0/44      Disabled
Ex0/45      Disabled
Ex0/46      Disabled
Ex0/47      Disabled
Ex0/48      Disabled
```

12.26 show port name

Displays the name of the specific interfaces.

show port name

Syntax Description	**n/a**
Mode	Privileged/User EXEC Mode
Package	Workgroup, Enterprise and Metro
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
Ex0/9        P9
Ex0/10       P10
Ex0/11       P11
Ex0/12       P12
Ex0/13       P13
Ex0/14       P14
Ex0/15       P15
Ex0/16       P16
Ex0/17       P17
Ex0/18       P18
Ex0/19       P19
Ex0/20       P20
```

Ex0/21	P21
Ex0/22	P22
Ex0/23	P23
Ex0/24	P24
Ex0/25	P25
Ex0/26	P26
Ex0/27	P27
Ex0/28	P28
Ex0/29	P29
Ex0/30	P30
Ex0/31	P31
Ex0/32	P32
Ex0/33	P33
Ex0/34	P34
Ex0/35	P35
Ex0/36	P36
Ex0/37	P37
Ex0/38	P38
Ex0/39	P39
Ex0/40	P40
Ex0/41	P41
Ex0/42	P42
Ex0/43	P43
Ex0/44	P44
Ex0/45	P45
Ex0/46	P46
Ex0/47	P47
Ex0/48	P48

12.27 show port description

Displays the description of the specific interfaces.

show port description

Syntax Description	**n/a**
Mode	Privileged/User EXEC Mode
Package	Workgroup, Enterprise and Metro
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
Ex0/9        Physical Port
Ex0/10       Physical Port
Ex0/11       Physical Port
Ex0/12       Physical Port
Ex0/13       Physical Port
Ex0/14       Physical Port
Ex0/15       Physical Port
Ex0/16       Physical Port
Ex0/17       Physical Port
Ex0/18       Physical Port
Ex0/19       Physical Port
Ex0/20       Physical Port
```

```
Ex0/21      Physical Port
Ex0/22      Physical Port
Ex0/23      Physical Port
Ex0/24      Physical Port
Ex0/25      Physical Port
Ex0/26      Physical Port
Ex0/27      Physical Port
Ex0/28      Physical Port
Ex0/29      Physical Port
Ex0/30      Physical Port
Ex0/31      Physical Port
Ex0/32      Physical Port
Ex0/33      Physical Port
Ex0/34      Physical Port
Ex0/35      Physical Port
Ex0/36      Physical Port
Ex0/37      Physical Port
Ex0/38      Physical Port
Ex0/39      Physical Port
Ex0/40      Physical Port
Ex0/41      Physical Port
Ex0/42      Physical Port
Ex0/43      Physical Port
Ex0/44      Physical Port
Ex0/45      Physical Port
Ex0/46      Physical Port
Ex0/47      Physical Port
Ex0/48      Physical Port
```

12.28 show parse-ip-header

Displays whether the parse-ip-header setting is enabled or disabled.

show parse-ip-header

Syntax Description	**n/a**
Mode	Privileged/User EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show parse-ip-header`
	`Parse IP Header : Enable`

12.29 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
Package	Workgroup, Enterprise and Metro
Example	`switch# show tagging-mode`
	`Tagging Mode : Single`

12.30 show cut-through global info

Displays global cut-through configuration.

show cut-through global info

Syntax Description	**n/a**
Mode	Privileged/User EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show cut-through global info`

```
Cut-Through mode disabled globally


 Minimal Packet Length 257
```

12.31 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
Package	Workgroup, Enterprise and Metro
Example	`switch# show in-traffic info`

```
Interface    Nested-Vlan
---------    -----------
Ex0/1        Disabled
Ex0/2        Disabled
Ex0/3        Disabled
Ex0/4        Disabled
Ex0/5        Disabled
Ex0/6        Disabled
Ex0/7        Disabled
Ex0/8        Disabled
Ex0/9        Disabled
Ex0/10       Disabled
Ex0/11       Disabled
Ex0/12       Disabled
Ex0/13       Disabled
Ex0/14       Disabled
Ex0/15       Disabled
Ex0/16       Disabled
Ex0/17       Disabled
Ex0/18       Disabled
Ex0/19       Disabled
Ex0/20       Disabled
```

```
Ex0/21      Disabled
Ex0/22      Disabled
Ex0/23      Disabled
Ex0/24      Disabled
Ex0/25      Disabled
Ex0/26      Disabled
Ex0/27      Disabled
Ex0/28      Disabled
Ex0/29      Disabled
Ex0/30      Disabled
Ex0/31      Disabled
Ex0/32      Disabled
Ex0/33      Disabled
Ex0/34      Disabled
Ex0/35      Disabled
Ex0/36      Disabled
Ex0/37      Disabled
Ex0/38      Disabled
Ex0/39      Disabled
Ex0/40      Disabled
Ex0/41      Disabled
Ex0/42      Disabled
Ex0/43      Disabled
Ex0/44      Disabled
Ex0/45      Disabled
Ex0/46      Disabled
Ex0/47      Disabled
Ex0/48      Disabled
```

12.32 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
Package	Workgroup, Enterprise and Metro
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
Ex0/9        allow
Ex0/10       allow
Ex0/11       allow
Ex0/12       allow
Ex0/13       allow
Ex0/14       allow
Ex0/15       allow
Ex0/16       allow
Ex0/17       allow
Ex0/18       allow
Ex0/19       allow
Ex0/20       allow
```

```
Ex0/21      allow
Ex0/22      allow
Ex0/23      allow
Ex0/24      allow
Ex0/25      allow
Ex0/26      allow
Ex0/27      allow
Ex0/28      allow
Ex0/29      allow
Ex0/30      allow
Ex0/31      allow
Ex0/32      allow
Ex0/33      allow
Ex0/34      allow
Ex0/35      allow
Ex0/36      allow
Ex0/37      allow
Ex0/38      allow
Ex0/39      allow
Ex0/40      allow
Ex0/41      allow
Ex0/42      allow
Ex0/43      allow
Ex0/44      allow
Ex0/45      allow
Ex0/46      allow
Ex0/47      allow
Ex0/48      allow
```

12.33 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
Package	Workgroup, Enterprise and Metro
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
Ex0/9        allow
Ex0/10       allow
Ex0/11       allow
Ex0/12       allow
Ex0/13       allow
Ex0/14       allow
Ex0/15       allow
Ex0/16       allow
Ex0/17       allow
Ex0/18       allow
Ex0/19       allow
Ex0/20       allow
```

```
Ex0/21      allow
Ex0/22      allow
Ex0/23      allow
Ex0/24      allow
Ex0/25      allow
Ex0/26      allow
Ex0/27      allow
Ex0/28      allow
Ex0/29      allow
Ex0/30      allow
Ex0/31      allow
Ex0/32      allow
Ex0/33      allow
Ex0/34      allow
Ex0/35      allow
Ex0/36      allow
Ex0/37      allow
Ex0/38      allow
Ex0/39      allow
Ex0/40      allow
Ex0/41      allow
Ex0/42      allow
Ex0/43      allow
Ex0/44      allow
Ex0/45      allow
Ex0/46      allow
Ex0/47      allow
Ex0/48      allow
```

12.34 show cut-through port-info

Displays cut-through information for a specific port.

show cut-through port-info

Syntax Description	**n/a**
Mode	Privileged/User EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show cut-through port-info`

```
Interface    Cut-Through-Mode  Rate-Limit
---------    ----------------  ----------
Ex0/1        Disabled          Disabled
Ex0/2        Disabled          Disabled
Ex0/3        Disabled          Disabled
Ex0/4        Disabled          Disabled
Ex0/5        Disabled          Disabled
Ex0/6        Disabled          Disabled
Ex0/7        Disabled          Disabled
Ex0/8        Disabled          Disabled
Ex0/9        Disabled          Disabled
Ex0/10       Disabled          Disabled
Ex0/11       Disabled          Disabled
Ex0/12       Disabled          Disabled
Ex0/13       Disabled          Disabled
Ex0/14       Disabled          Disabled
Ex0/15       Disabled          Disabled
Ex0/16       Disabled          Disabled
Ex0/17       Disabled          Disabled
Ex0/18       Disabled          Disabled
Ex0/19       Disabled          Disabled
Ex0/20       Disabled          Disabled
```

Ex0/21	Disabled	Disabled
Ex0/22	Disabled	Disabled
Ex0/23	Disabled	Disabled
Ex0/24	Disabled	Disabled
Ex0/25	Disabled	Disabled
Ex0/26	Disabled	Disabled
Ex0/27	Disabled	Disabled
Ex0/28	Disabled	Disabled
Ex0/29	Disabled	Disabled
Ex0/30	Disabled	Disabled
Ex0/31	Disabled	Disabled
Ex0/32	Disabled	Disabled
Ex0/33	Disabled	Disabled
Ex0/34	Disabled	Disabled
Ex0/35	Disabled	Disabled
Ex0/36	Disabled	Disabled
Ex0/37	Disabled	Disabled
Ex0/38	Disabled	Disabled
Ex0/39	Disabled	Disabled
Ex0/40	Disabled	Disabled
Ex0/41	Disabled	Disabled
Ex0/42	Disabled	Disabled
Ex0/43	Disabled	Disabled
Ex0/44	Disabled	Disabled
Ex0/45	Disabled	Disabled
Ex0/46	Disabled	Disabled
Ex0/47	Disabled	Disabled
Ex0/48	Disabled	Disabled

12.35 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
Package	Workgroup, Enterprise and Metro
Example	`switch# show global hash-mode`

```
Hash-mode: packet-xor
```

12.36 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
Package	Workgroup, Enterprise and Metro
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

12.37 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
Package	Workgroup, Enterprise and Metro
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
Ex0/9        Enabled           0
Ex0/10       Enabled           0
Ex0/11       Enabled           0
Ex0/12       Enabled           0
Ex0/13       Enabled           0
Ex0/14       Enabled           0
Ex0/15       Enabled           0
Ex0/16       Enabled           0
Ex0/17       Enabled           0
Ex0/18       Enabled           0
Ex0/19       Enabled           0
```

```
Ex0/20      Enabled          0
Ex0/21      Enabled          0
Ex0/22      Enabled          0
Ex0/23      Enabled          0
Ex0/24      Enabled          0
Ex0/25      Enabled          0
Ex0/26      Enabled          0
Ex0/27      Enabled          0
Ex0/28      Enabled          0
Ex0/29      Enabled          0
Ex0/30      Enabled          0
Ex0/31      Enabled          0
Ex0/32      Enabled          0
Ex0/33      Enabled          0
Ex0/34      Enabled          0
Ex0/35      Enabled          0
Ex0/36      Enabled          0
Ex0/37      Enabled          0
Ex0/38      Enabled          0
Ex0/39      Enabled          0
Ex0/40      Enabled          0
Ex0/41      Enabled          0
Ex0/42      Enabled          0
Ex0/43      Enabled          0
Ex0/44      Enabled          0
Ex0/45      Enabled          0
Ex0/46      Enabled          0
Ex0/47      Enabled          0
Ex0/48      Enabled          0
```

12.38 show force-link-up info

Displays the force link up status of all ports.

show force-link-up info

Syntax Description	**n/a**
Mode	Privileged/User EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show force-link-up info`

```
Interface    Force 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
Ex0/9        Disabled
Ex0/10       Disabled
Ex0/11       Disabled
Ex0/12       Disabled
Ex0/13       Disabled
Ex0/14       Disabled
Ex0/15       Disabled
Ex0/16       Disabled
Ex0/17       Disabled
Ex0/18       Disabled
Ex0/19       Disabled
Ex0/20       Disabled
```

```
Ex0/21      Disabled
Ex0/22      Disabled
Ex0/23      Disabled
Ex0/24      Disabled
Ex0/25      Disabled
Ex0/26      Disabled
Ex0/27      Disabled
Ex0/28      Disabled
Ex0/29      Disabled
Ex0/30      Disabled
Ex0/31      Disabled
Ex0/32      Disabled
Ex0/33      Disabled
Ex0/34      Disabled
Ex0/35      Disabled
Ex0/36      Disabled
Ex0/37      Disabled
Ex0/38      Disabled
Ex0/39      Disabled
Ex0/40      Disabled
Ex0/41      Disabled
Ex0/42      Disabled
Ex0/43      Disabled
Ex0/44      Disabled
Ex0/45      Disabled
Ex0/46      Disabled
Ex0/47      Disabled
Ex0/48      Disabled
```

12.39 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
Package	Workgroup, Enterprise and Metro
Example	`switch# show filter-match poll-time-interval`

```
Filter-Hits Poll-Time-Interval : 1 Second
```

12.40 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
Package	Workgroup, Enterprise and Metro
Example	`switch# show filter-match count`

```
Filter   Filter-Type  Match-Pkt-Count     Match-Byte-Count
Bits/Sec

------   -----------  -----------------   -----------------  --
------

1001      IP                0                              0
```

12.41 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
Package	Workgroup, Enterprise and Metro
Example	`switch# clear filter-match type ip`

12.42 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
Package	Workgroup, Enterprise and Metro
Example	`switch# show port-group`

```
Id              : 49
Type            : Port Channel
Name            : PO49
Desc            : Enter description here
Ports           : Ex0/1, Ex0/2
-----------------------------------------------
```

12.43 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

Package Workgroup, Enterprise and Metro

Example

```
switch# show configuration map all

-----------------------------------------------
Config Map                      : 1
Input Ports                     : Ex0/1
Output Ports                    : Ex0/2

IP Filter's                     : 1001
Filter Priority                 : 2998
Description                     : Enter description here
Name                            : New Configuration Map
Status                          : Enabled
Advance Action                  : None
Filter Mode                     : Pass All
```

12.44 show tech-support

Displays debug information which can be used for technical support should it be required.

show tech-support

Syntax Description	**n/a**
Mode	Privileged/User EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	`switch# show tech-support`

```
 ============================

 ============================

 ============================

 ============================

 ============================

 ============================

 ============================
Port 1 Nested Vlan Disable
Port 2 Nested Vlan Disable
Port 3 Nested Vlan Disable
Port 4 Nested Vlan Disable
Port 5 Nested Vlan Disable
Port 6 Nested Vlan Disable
Port 7 Nested Vlan Disable
Port 8 Nested Vlan Disable
Port 9 Nested Vlan Disable
Port 10 Nested Vlan Disable
Port 11 Nested Vlan Disable
Port 12 Nested Vlan Disable
Port 13 Nested Vlan Disable
Port 14 Nested Vlan Disable
Port 15 Nested Vlan Disable
Port 16 Nested Vlan Disable
Port 17 Nested Vlan Disable
Port 18 Nested Vlan Disable
Port 19 Nested Vlan Disable
```

```
Port 20 Nested Vlan Disable
Port 21 Nested Vlan Disable
Port 22 Nested Vlan Disable
Port 23 Nested Vlan Disable
Port 24 Nested Vlan Disable

Trunk Id = 1 ports  62
Trunk Id = 2 ports  62
Trunk Id = 3 ports  62
Trunk Id = 4 ports  62
Trunk Id = 5 ports  62
Trunk Id = 6 ports  62
Trunk Id = 7 ports  62
Trunk Id = 8 ports  62
Trunk Id = 9 ports  62
Trunk Id = 10 ports  62
Trunk Id = 11 ports  62
Trunk Id = 12 ports  62
Trunk Id = 13 ports  62
Trunk Id = 14 ports  62
Trunk Id = 15 ports  62
Trunk Id = 16 ports  62
Trunk Id = 17 ports  62
Trunk Id = 18 ports  62
Trunk Id = 19 ports  62
Trunk Id = 20 ports  62
Trunk Id = 21 ports  62
Trunk Id = 22 ports  62
Trunk Id = 23 ports  62
Trunk Id = 24 ports  62
Trunk Id = 25 ports  62
Trunk Id = 26 ports  62
Trunk Id = 27 ports  62
Trunk Id = 28 ports  62
Trunk Id = 29 ports  62
Trunk Id = 30 ports  62
Trunk Id = 31 ports  62
```

```
Trunk Id = 32 ports  62
Trunk Id = 33 ports  62
Trunk Id = 34 ports  62
Trunk Id = 35 ports  62
Trunk Id = 36 ports  62
Trunk Id = 37 ports  62
Trunk Id = 38 ports  62
Trunk Id = 39 ports  62
Trunk Id = 40 ports  62
Trunk Id = 41 ports  62
Trunk Id = 42 ports  62
Trunk Id = 43 ports  62
Trunk Id = 44 ports  62
Trunk Id = 45 ports  62
Trunk Id = 46 ports  62
Trunk Id = 47 ports  62
Trunk Id = 48 ports  62
Trunk Id = 49 ports  62
Trunk Id = 50 ports  62
Trunk Id = 51 ports  62
Trunk Id = 52 ports  62
Trunk Id = 53 ports  62
Trunk Id = 54 ports  62
Trunk Id = 55 ports  62
Trunk Id = 56 ports  62
Trunk Id = 57 ports  62
Trunk Id = 58 ports  62
Trunk Id = 59 ports  62
Trunk Id = 60 ports  62
Trunk Id = 61 ports  62
Trunk Id = 62 ports  62
Trunk Id = 63 ports  62
Trunk Id = 64 ports  62
Trunk Id = 65 ports  62
Trunk Id = 66 ports  62
Trunk Id = 67 ports  62
Trunk Id = 68 ports  62
```

```
Trunk Id = 69 ports  62
Trunk Id = 70 ports  62
Trunk Id = 71 ports  62
Trunk Id = 72 ports  62
Trunk Id = 73 ports  62
Trunk Id = 74 ports  62
Trunk Id = 75 ports  62
Trunk Id = 76 ports  62
Trunk Id = 77 ports  62
Trunk Id = 78 ports  62
Trunk Id = 79 ports  62
Trunk Id = 80 ports  62
Trunk Id = 81 ports  62
Trunk Id = 82 ports  62
Trunk Id = 83 ports  62
Trunk Id = 84 ports  62
Trunk Id = 85 ports  62
Trunk Id = 86 ports  62
Trunk Id = 87 ports  62
Trunk Id = 88 ports  62
Trunk Id = 89 ports  62
Trunk Id = 90 ports  62
Trunk Id = 91 ports  62
Trunk Id = 92 ports  62
Trunk Id = 93 ports  62
Trunk Id = 94 ports  62
Trunk Id = 95 ports  62
Trunk Id = 96 ports  62
Trunk Id = 97 ports  62
Trunk Id = 98 ports  62
Trunk Id = 98 ports  62
Trunk Id = 99 ports  62
Trunk Id = 100 ports  62
Trunk Id = 101 ports  62
Trunk Id = 102 ports  62
Trunk Id = 103 ports  62
Trunk Id = 104 ports  62
```

```
Trunk Id = 105 ports  62
Trunk Id = 106 ports  62
Trunk Id = 107 ports  62
Trunk Id = 108 ports  62
Trunk Id = 109 ports  62
Trunk Id = 110 ports  62
Trunk Id = 111 ports  62
Trunk Id = 112 ports  62
Trunk Id = 113 ports  62
Trunk Id = 114 ports  62
Trunk Id = 115 ports  62
Trunk Id = 116 ports  62
Trunk Id = 117 ports  62
Trunk Id = 118 ports  62
Trunk Id = 119 ports  62
Trunk Id = 120 ports  62
Trunk Id = 121 ports  62
Trunk Id = 122 ports  62
Trunk Id = 123 ports  62
Trunk Id = 124 ports  62
Trunk Id = 125 ports  62
Trunk Id = 126 ports  62
Trunk Id = 127 ports  62
 Ip Mode = 0
 Mac  Mode = 0
 IPv6 Mode = 3
L4 Mode Disabled
 MPLS Global Mode = 0
CPSS_DXCH_TRUNK_LBH_MASK_MAC_DA_E mask = 0x3f
CPSS_DXCH_TRUNK_LBH_MASK_MAC_SA_E mask = 0x3f
CPSS_DXCH_TRUNK_LBH_MASK_MPLS_LABEL0_E mask = 0x3f
CPSS_DXCH_TRUNK_LBH_MASK_MPLS_LABEL1_E mask = 0x3f
CPSS_DXCH_TRUNK_LBH_MASK_MPLS_LABEL2_E mask = 0x3f
CPSS_DXCH_TRUNK_LBH_MASK_IPV4_DIP_E mask = 0x3f
CPSS_DXCH_TRUNK_LBH_MASK_IPV4_SIP_E mask = 0x3f
CPSS_DXCH_TRUNK_LBH_MASK_IPV6_DIP_E mask = 0x3f
CPSS_DXCH_TRUNK_LBH_MASK_IPV6_SIP_E mask = 0x3f
```

```
CPSS_DXCH_TRUNK_LBH_MASK_IPV6_FLOW_E mask = 0x3f
CPSS_DXCH_TRUNK_LBH_MASK_L4_DST_PORT_E mask = 0x3f
CPSS_DXCH_TRUNK_LBH_MASK_L4_SRC_PORT_E mask = 0x3f
SOURCE IP is Cyclic Left Shift by 0 Byte
Destination IP is Cyclic Left Shift by 0 Byte
<cpssDxChBrgVlanEntryRead> returned 4, exiting----------------
---
HwId        SwId     Inport    Type    Out/sid   cpucode src-ip
smask           dst-ip      dmask
====        ====     ======    ====    =======   ======= ======
=====           ======      =====

 Total MAC Rules in hardware         :0
 Total IP Rules in hardware          :0
 Total UDB Rules in hardware         :0
 Total Egress MAC Rules in hardware  :0
 Total Egress IP Rules in hardware   :0
HwId      SwId    Inport   OutPort  Type
====      ====    ======   =======  ====
 Total Tunnel Rules in hardware         :0
Port 1 Admin Status UP   Link Status DOWN
Port 2 Admin Status UP   Link Status DOWN
Port 3 Admin Status UP   Link Status DOWN
Port 4 Admin Status UP   Link Status DOWN
Port 5 Admin Status UP   Link Status DOWN
Port 6 Admin Status UP   Link Status DOWN
Port 7 Admin Status UP   Link Status DOWN
Port 8 Admin Status UP   Link Status DOWN
Port 9 Admin Status UP   Link Status DOWN
Port 10 Admin Status UP   Link Status DOWN
Port 11 Admin Status UP   Link Status DOWN
Port 12 Admin Status UP   Link Status DOWN
Port 13 Admin Status UP   Link Status DOWN
Port 14 Admin Status UP   Link Status DOWN
Port 15 Admin Status UP   Link Status DOWN
Port 16 Admin Status UP   Link Status DOWN
Port 17 Admin Status UP   Link Status DOWN
Port 18 Admin Status UP   Link Status DOWN
Port 19 Admin Status UP   Link Status DOWN
```

```
Port 20 Admin Status UP   Link Status DOWN
Port 21 Admin Status UP   Link Status DOWN
Port 22 Admin Status UP   Link Status DOWN
Port 23 Admin Status UP   Link Status DOWN
Port 24 Admin Status UP   Link Status DOWN
Port 25 Admin Status UP   Link Status DOWN
Port 26 Admin Status UP   Link Status DOWN
Port 27 Admin Status UP   Link Status DOWN
Port 28 Admin Status UP   Link Status DOWN
Port 29 Admin Status UP   Link Status DOWN
Port 30 Admin Status UP   Link Status DOWN
Port 31 Admin Status UP   Link Status DOWN
Port 32 Admin Status UP   Link Status DOWN
Port 33 Admin Status UP   Link Status DOWN
Port 34 Admin Status UP   Link Status DOWN
Port 35 Admin Status UP   Link Status DOWN
Port 36 Admin Status UP   Link Status DOWN
Port 37 Admin Status UP   Link Status DOWN
Port 38 Admin Status UP   Link Status DOWN
Port 39 Admin Status UP   Link Status DOWN
Port 40 Admin Status UP   Link Status DOWN
Port 41 Admin Status UP   Link Status DOWN
Port 42 Admin Status UP   Link Status DOWN
Port 43 Admin Status UP   Link Status DOWN
Port 44 Admin Status UP   Link Status DOWN
Port 45 Admin Status UP   Link Status DOWN
Port 46 Admin Status UP   Link Status DOWN
Port 47 Admin Status UP   Link Status DOWN
Port 48 Admin Status UP   Link Status DOWN

Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel System Identifier is  00:00:bd:72:91:f0
```

```
Vlan database
-------------
Vlan ID             : 1
Member Ports        : None
Untagged Ports      : None
Forbidden Ports     : None
Name                :
Status              : Permanent
-----------------------------------------------------


IP ACCESS LISTS
-----------------
 No IP Access Lists have been configured

MAC ACCESS LISTS
-----------------

 No MAC Access Lists have been configured


USER DEFINED LISTS
----------------------

 No User Defined Lists have been configured

Hardware Version                 : 5.5.5
Firmware Version                 : XXXXX_7.6-13
Switch Name                      : SWITCH
System Contact                  : support@garlandtechnology.com
System Location                 : Garland Technology LLC
Logging Option                   : Console Logging
Login Authentication Mode        : Local
Config Save Status               : Not Initiated
Remote Save Status               : Not Initiated
Config Restore Status            : Not Initiated
```

```
Egress Filtering                    : Enabled
Provision mode                      : Consolidated
Telnet                              : Enabled
Backward-Compatibility              : Disabled
Auto-Hw-Programmming                : Enabled


Interface    Status   Protocol
---------    ------   --------
Ex0/1        up       down
Ex0/2        up       down
Ex0/3        up       down
Ex0/4        up       down
Ex0/5        up       down
Ex0/6        up       down
Ex0/7        up       down
Ex0/8        up       down
Ex0/9        up       down
Ex0/10       up       down
Ex0/11       up       down
Ex0/12       up       down
Ex0/13       up       down
Ex0/14       up       down
Ex0/15       up       down
Ex0/16       up       down
Ex0/17       up       down
Ex0/18       up       down
Ex0/19       up       down
Ex0/20       up       down
Ex0/21       up       down
Ex0/22       up       down
Ex0/23       up       down
Ex0/24       up       down
Ex0/25       up       down
Ex0/26       up       down
Ex0/27       up       down
Ex0/28       up       down
```

```
Ex0/29          up          down
Ex0/30          up          down
Ex0/31          up          down
Ex0/32          up          down
Ex0/33          up          down
Ex0/34          up          down
Ex0/35          up          down
Ex0/36          up          down
Ex0/37          up          down
Ex0/38          up          down
Ex0/39          up          down
Ex0/40          up          down
Ex0/41          up          down
Ex0/42          up          down
Ex0/43          up          down
Ex0/44          up          down
Ex0/45          up          down
Ex0/46          up          down
Ex0/47          up          down
Ex0/48          up          down
cpu0            up          up
```

12.45 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		
Package	Workgroup, Enterprise and Metro		

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
Extended IP Access List 10022
-----------------------------
 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
```

☞

- OuterEtherType, Service Vlan, Service Vlan Priority, innerEtherType, Customer Vlan and Customer Vlan Priority options are applicable only with Metro Ethernet Feature and bridge mode is provider.

12.46 HTTPS

The following section will detail how to enable HTTPS functionality and access to the management port. A Linux server is required to generate the certificate.

- **Create a self signed certificate for the Certification Authority (CA). This is the command done in Linux.**

  openssl req -x509 -newkey rsa:1024 -keyout key_file.pem -out ca_file.pem

  →command will generate RSA key pair of 1024 Bits.

  →pass phase is an mandatory.

- **Generate RSA key pair for server. The key can be either 512 bits or 1024 bits. This is done on the FAB.**
  1. **switch(config)#** ***ip http secure crypto key rsa 1024***
  2. **switch#** ***ssl gen cert-req algo rsa sn name <name different from pass phrase>***

  copy the generated certificate to file named cert_req.pem

- **To Generate Public certificate of SSL_SERVER to be imported by the below command. This command is done in Linux**

openssl x509 -req -in cert_req.pem -out pcert_file.pem -CA ca_file.pem -CAkey key_file.pem –Cacreateserial

This command will generate pcert_file.pem→ Remove all new line and copy it.

- **Import pcert_file.pem to SSL_SERVER. This is done on the FAB.**

  switch# ***ssl server-cert***

  →it will prompt for the certificate paste the above copied pcert_file.pem

- **To enable https server, give the following command in SWITCH. This is done on the FAB.**

  switch(config)# ip http secure server

DOCUMENT No.: Garland Technology FAB-CLI_v2.0-GT-rev2

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