D-Link®
Building Networks for People

DES-1210-10/28

CLI Reference Guide
Web Smart Switch

Table of Contents

About This Guide

This guide introduces the D-Link Fast Ethernet Web Smart Switch DES-1210-10 and DES-1210-28.

The Switch can be configured and managed via the Telnet interfaces. This manual provides instructions and a reference for all of the commands contained in the CLI.

Note: The model you have purchased may appear slightly different from the illustrations shown in the document. Refer to the Product Instruction and Technical Specification sections for detailed information about your switch, its components, network connections, and technical specifications.

Copyright and Trademarks

1 INTRODUCTION

The D-Link Web Smart Switch allows a computer or terminal to perform some basic monitoring and configuration tasks by using the Command Line Interface (CLI) via TELNET protocol.

To connect a switch via TELNET:

1. Make sure the network connection between the switch and PC is active.
2. To connect, launch any terminal software like ***HyperTerminal*** in Microsoft Windows, or just use the command prompt by typing the command *telnet* followed by the switch IP address, eg. *telnet 10.90.90.90*.
3. The logon prompt will appear.

Logging on to the Command Line Interface:

Enter your User Name and Password to log in. The default user name and password is **null**. Press **Enter** in both the Username and Password fields. The command prompt will appear as shown below:

```
                    DES-1210-10 Fast Ethernet Switch
                            Command Line Interface

                           Firmware: Build 5.20.009
             Copyright(C) 2010 D-Link Corporation. All rights reserved.
DES-1210-10 login:
Password:

DES-1210-10:5#
```

Figure 1 DES-1210-10 Command Prompt

```
                    DES-1210-28 Fast Ethernet Switch
                            Command Line Interface

                           Firmware: Build 5.20.009
             Copyright(C) 2010 D-Link Corporation. All rights reserved.
DES-1210-28 login:
Password:

DES-1210-28:5#
```

Figure 2 DES-1210-28 Command Prompt

The user session is automatically terminated if idle for the login timeout period. The default login timeout period is 5 minutes.

2 *COMMAND SYNTAX*

The following symbols are used to describe how command entries are made and values and arguments are specified in this manual. The online help contained in the CLI and available through the console interface uses the same syntax.

Note: All commands are case-sensitive. Be sure to disable Caps Lock or any other unwanted function that changes text case.

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	create account [admin | operator |user] <username 15>
Description	In the above syntax example, supply a username in the <username> space. Do not type the angle brackets.
Example Command	create account admin newadmin1

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One value or argument can be specified.
Syntax	create account [admin | operator |user] <username 15>
Description	In the above syntax example, specify admin, oper or a user level account to be created. Do not type the square brackets.
Example Command	create account user newuser1

| vertical bar	
Purpose	Separates two or more mutually exclusive items in a list, one of which must be entered.
Syntax	create account [admin | operator | user] <username 15>
Description	In the above syntax example, specify admin, oper, or user. Do not type the vertical bar.
Example Command	create account user newuser1

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
Syntax	reset
Description	Execute “reset” will return the switch to its factory default setting.
Example command	reset Please be aware that all configuration will be reset to default value. Are you sure you want to proceed with system reset now? (Y/N)[N] N

3 *BASIC SWITCH Commands*

The Basic Switch commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) below.

Command	Parameter
create account	create account [admin | operator | user] <username 15> {password <password_string> {encrypted}}
config account	config account <username 15>
show account	
show session	
show switch	
enable clipaging	
enable clipaging	
disable clipaging	
delete account	delete account <username 15>
enable web	enable web <tcp_port_number 1-65535>
disable web	
save	save {[config config_id<value 1-2> | log]}
reboot	
reset config	
logout	
enable autoconfig	
disable autoconfig	
show autoconfig	
ping	ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
enable dhcp_relay	
disable dhcp_relay	
show dhcp_relay	

Each command is listed in detail, as follows:

create account

The **create account** command creates an administrator, operator, or user account that consists of a username and an optional password. Up to 31 accounts can be created. You can enter username and Enter. In this case, the system prompts for the account's password, which may be between 0 and 15 characters. Alternatively, you can enter the username and password on the same line.

create account	
Syntax	**create account [admin | operator | user] <username 15> {password <password_string> {encrypted}}**
Parameter	*admin* − Creates an administrator account. *operator* − Creates an operator account. *user* − Creates a user account with read-only permissions. <*username 1-15*> − The account username may be between 1 and 15 characters. *password* <password_string> {encrypted} - the account password can

be included, and (optionally) can be encrypted.

config account

The **config account** command changes the password for a user account that has been created using the **create account** command. The system prompts for the account's new password, which may be between 0 and 15 characters.

config account	
Syntax	**config account <username 15>**
Parameter	*<username 1-15>* − The account username.

show account

The **show account** command displays all account usernames and their access levels created on the Switch. Up to 31 user accounts can exist on the Switch at one time.

show account	
Syntax	**show account**
Parameter	None.

show session

The **show session** command displays a list of all the users that are logged-in at the time the command is issued. The information includes the session ID (0 for the first logged-in user, 1 for the next logged-in user, etc.), the Protocol used to connect to the Switch, the user's IP address, the user's access Level (1=user, 15=admin), and the account name on the Switch.

show session	
Syntax	**show session**
Parameter	None.

show switch

The **show switch** command displays information about the Switch settings, including Device Type, MAC Address, IP configuration, Hardware/Software version, System information, and Switch Network configuration.

show switch	
Syntax	**show switch**
Parameter	None.

enable clipaging

The **enable clipaging** command pauses the scrolling of the console screen at the end of each page when issuing a command which would display more than one screen of information. The default setting is enabled.

enable clipaging	
Syntax	**enable clipaging**
Parameter	None.

disable clipaging

To disable the pausing of the console screen scrolling at the end of each page when the command displays more than one screen of information.

disable clipaging

Syntax	**disable clipaging**
Parameter	None.

delete account

The **delete account** command deletes a user account that has been created using the **create account** command.

delete account	
Syntax	**delete account <username 15>**
Parameter	*<username 1-15>* − the account username.

enable web

The **enable web** command enables the Web-based management software on the Switch. The user can specify the TCP port number the Switch uses to listen for Telnet requests.

enable web	
Syntax	**enable web <tcp_port_number 1-65535>**
Parameter	*<tcp_port_number 1-65535>* − The TCP port number. TCP ports are numbered between 1 and 65535. The 'well-known' port for the Web-based management software is 80.

disable web

The **disable web** command disables the Web-based management software on the Switch.

disable web	
Syntax	**disable web**
Parameter	None.

save

The **save** command saves the current switch configuration or log to non-volatile RAM. The saved switch configuration or log is loaded to the Switch's memory each time the Switch is restarted.

save	
Syntax	**save {[config config_id<value 1-2> | log]}**
Parameter	*config_id<value 1-2>* − Specify to save current settings to configuration file 1 or 2. *log* − Specify to save current Switch log to NV-RAM.

reboot

The **reboot** command restarts the Switch.

reboot	
Syntax	**reboot**
Parameter	None.

reset config

The **reset config** command restores the Switch's configuration to the default settings assigned from the factory.

reset config	
Syntax	**reset config**

Parameter	None.

logout

The **logout** command terminates the current user's session on the Switch's console.

logout	
Syntax	**logout**
Parameter	None.

enable autoconfig

The **enable autoconfig** command is used to activate the auto configuration function for the Switch. This will load a configuration from the TFTP server specified in the reply.

enable autoconfig	
Syntax	**enable autoconfig**
Parameter	None.

disable autoconfig

The **disable autoconfig** command is used to disable the auto configuration function for the Switch.

disable autoconfig	
Syntax	**disable autoconfig**
Parameter	None.

show autoconfig

The **show autoconfig** command is used to display the current auto configuration status on the Switch.

show autoconfig	
Syntax	**show autoconfig**
Parameter	None.

ping

The **ping** command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address then 'echos' or returns the message. This is used to confirm connectivity between the Switch and the remote device.

ping	
Syntax	**ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}**
Parameter	*<ipaddr>* - The IP address of the host. *times <value 1-255>* - The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 4. *timeout <sec 1-99>* - The time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second.

enable dhcp_relay

The **enable dhcp_relay** command sets the DHCP Relay to be globally enabled on the Switch and on all existing VLANs.

enable dhcp_relay

Syntax	**enable dhcp_relay**
Parameter	None.

disable dhcp_relay

The **disable dhcp_relay** command sets the DHCP Relay to be globally disabled on the Switch and on all existing VLANs.

disable dhcp_relay	
Syntax	**disable dhcp_relay**
Parameter	None.

show dhcp_relay

The **show dhcp_relay** command sets the DHCP Relay to be globally disabled on the Switch and on all existing VLANs.

show dhcp_relay	
Syntax	**show dhcp_relay**
Parameter	None.

4 SMTP SERVER Commands

The SMTP Server commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters).

Command	Parameter
enable smtp	
disable smtp	
config smtp	config smtp [self_mail_addr <mail_addr 64> | server <ipaddr> | server_port <tcp_port_number 1-65535>] [{add mail_receiver <mail_addr 64>| delete mail_receiver <index 1-8> }]
show smtp	
smtp sent_testmsg	

Each command is listed in detail, as follows:

enable smtp

The **enable smtp** command enables the SMTP server feature on the Switch.

enable smtp	
Syntax	**enable smtp**
Parameter	None.

disable smtp

The **disable smtp** command disables the SMTP server feature on the Switch.

disable smtp	
Syntax	**disable smtp**
Parameter	None.

config smtp

The **config smtp** command is used to configure the fields to set up the SMTP server for the switch, along with setting e-mail addresses to which switch log files can be sent when a problem arises on the Switch.

config smtp	
Syntax	**config smtp [self_mail_addr <mail_addr 64> | server <ipaddr> | server_port <tcp_port_number 1-65535>] [{add mail_receiver <mail_addr 64>| delete mail_receiver <index 1-8> }]**
Parameter	*self_mail_addr <mail_addr 64>* − Specifies the e-mail address from which mail messages will be sent. Only one self mail address can be configured on the Swtich. *server <ipaddr>* − Specifies the IP address of the SMTP server. This will be the device that sends out the mail for user. For example, 10.90.90.99. *<tcp_port_number 1-65535>* − Specifies the port number that the Switch will connect with on the SMTP server. The range is between 1 and 65535. *add mail_receiver <mail_addr 64>* − Specifies a list of e-mail addresses so recipients can receive e-mail messages regarding Switch functions. Up to 8 e-mail address can be added per Switch. *delete mail_receiver <index 1-8>* − Specifies the e-mail address index

to be deleted.

show smtp

The **show smtp** command displays the SMTP server settings on the Switch.

show smtp	
Syntax	**show smtp**
Parameter	None.

smtp sent_testmsg

The **smtp sent_testmsg** command is used to send test messages to all mail recipients configured on the Switch.

smtp sent_testmsg	
Syntax	**smtp sent_testmsg**
Parameter	None.

5 SWITCH PORT Commands

The Switch Port commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters).

Command	Parameter
config ports	config ports [all | <portlist>] medium_type [copper | fiber_100 | fiber 1G] {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full] | description <desc 32> | flow_control [enable | disable] | MDI/MDIX | state [enable | disable]}
show ports	show ports {<portlist> | all | description | err_disabled}

Each command is listed in detail, as follows:

config ports

The **config ports** command configures the Switch's Ethernet port settings.

config ports	
Syntax	**config ports [all | <portlist>] medium_type [copper | fiber_100 | fiber 1G] {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full] | description <desc 32> | flow_control [enable | disable] | MDI/MDIX | state [enable | disable]}**
Parameter	*<portlist>* − A port or range of ports to be configured. For example, 2 or 2-8 or 2,4,6. *all* − Configures all ports on the Switch. *medium_type* − Specifies the medium type to be copper, fiber 100M or fiber 1G. *speed* – Sets the speed of a port or range of ports, with the addition of one of the following: • *auto* − Enables auto-negotiation for the specified range of ports. • *[10 | 100 | 1000]* − Configures the speed in Mbps for the specified range of ports. • *[half | full]* − Configures the specified range of ports as either full or half-duplex. *description <desc 32>* – Specifies the description content for the port. *flow_control [enable]* – Enables flow control for the specified ports. *flow_control [disable]* – Disables flow control for the specified ports. MDI/MDIX − Displayed the MDI or MDIX status for the specified ports. *state [enable | disable]* − Enables or disables the specified range of ports.

show ports

The **show ports** command displays the current configuration of a port or range of ports.

show ports	
Syntax	**show ports {<portlist> | all | description | err_disabled}**
Parameter	*<portlist>* − A port or range of ports whose settings are to be displayed. *all* − All ports settings are to be displayed. *description* − Displays the description for the ports. *err_disabled* − Displays the information about ports that have had their connection status disabled, for reasons such as STP loopback detection or link down status.

6 LOOPBACK DETECTION Commands

The Loopback Detection commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters).

Command	Parameter
config loopdetect	config loopdetect {ports [<portlist> | all] [disable | enable]}
confit loopdetect	config loopdetect {interval_time <value 1-32767> lbd_recover_time [0 | <value 60-10000>]}

Each command is listed in detail, as follows:

config loopdetect

The **config loopdetect** command configures the loop back detection to be enabled or disabled on the Switch.

config loopdetect	
Syntax	**config loopdetect {ports [<portlist> | all] [disable | enable]}**
Parameter	*<portlist>* − A port or range of ports to be configured. *all* − All ports settings are to be configured. *[enabled | disabled]* − Specifies the loop back detection is enabled or disabled for the specified ports on the Switch.

config loopdetect

The **config loopdetect** command configures the loop back detection to be enabled or disabled on the Switch.

config loopdetect	
Syntax	**config loopdetect {interval_time <value 1-32767> lbd_recover_time [0 | <value 60-10000>]}**
Parameter	*interval_time <value 1-32767>* − Specifies the interval time of loop back detection. The range is between 1 and 32767 seconds. *lbd_recover_time [0 | <value 60-10000>]* − Specifies the recover time of loop back detection on the switch. The range is between 60 and 10000 seconds.

7 NETWORK MANAGEMENT (SNMP) Commands

The Network Management (SNMP) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters).

Command	Parameter
create snmp user	<username 32> <groupname 32> [v1 | v2c | v3] [md5 <auth_password 32> | sha <auth_password 32>] | [DES <priv_password 32> | none]
delete snmp user	<username 32>
show snmp user	
create snmp view	<view_name 32> <oid 32> <oid mask 32> view_type [included | excluded]
delete snmp view	<view_name 32> <oid 32>
show snmp view	<view_name 32>
create snmp community	<community_string 20> <username 32>
delete snmp community	<community_string 32>
show snmp community	<community_string 32>
config snmp engineID	<snmp_engineID 64>
show snmp engineID	
create snmp group	<groupname 32> [v1 | v2c | v3] {notify_view <view_name 32>} {read_view <view_name 32> | write_view <view_name 32>}
delete snmp group	<groupname 32>
show snmp groups	
create snmp host	<ipaddr> [v1<username 32> | v2c<username 32> | v3 [noauth_nopriv | auth_nopriv | auth_priv]<username 32>]
delete snmp host	<ip_addr>
show snmp host	<ip_addr>
enable snmp traps	
disable snmp traps	
enable snmp authenticate traps	
disable snmp authenticate traps	
show snmp traps	
enable snmp	
disable snmp	
enable snmp system_device_bootup traps	
disable snmp system_device_bootup traps	
enable snmp fiber_port_link traps	

disable snmp fiber_port_link traps

enable snmp firmware_upgrade_state traps

disable snmp firmware_upgrade_state traps

enable snmp rstpport_state_change traps

disable snmp rstpport_state_change traps

Each command is listed in detail, as follows:

create snmp user

The **create snmp user** command creates a new SNMP user and adds the user to an existing SNMP group.

create snmp user	
Syntax	**create snmp user <username 32> <groupname 32> [v1 | v2c | v3] [md5 <auth_password 32> | sha <auth_password 32>] | [DES <priv_password 32> | none]**
Parameter	*<username 32>* − The new SNMP username, up to 32 alphanumeric characters. *<groupname 32>* − The SNMP groupname the new SNMP user is associated with, up to 32 alphanumeric characters. *v1* – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: Message integrity − Ensures that packets have not been tampered with during transit. Authentication − Determines if an SNMP message is from a valid source. Encryption − Scrambles the contents of messages to prevent it from being viewed by an unauthorized source. The user may also choose the type of authentication algorithms used to authenticate the snmp user. The choices are: *md5* − Specifies that the HMAC-MD5-96 authentication level to be used. *sha* − Specifies that the HMAC-SHA-96 authentication level will be used. <auth_password 32> − A string of between 1 and 32 alphanumeric characters used to authorize the agent to receive packets for the host.

delete snmp user

The **delete snmp user** command removes an SNMP user from its SNMP group and then deletes the associated SNMP group.

delete snmp user	
Syntax	**delete snmp user <username 32>**
Parameter	<*username 32*> − A string of up to 2324 alphanumeric characters that identifies the SNMP user to be deleted.

show snmp user

The **show snmp user** command displays information about each SNMP username in the SNMP group username table.

show snmp user	
Syntax	**show snmp user**
Parameter	None.

create snmp view

The **create snmp view** command assigns views to community strings to limit which MIB objects an SNMP manager can access.

create snmp view	
Syntax	**create snmp view <view_name 32> <oid 32> <oid mask 32> view_type [included | excluded]**
Parameter	<*view_name 32*> − A string of up to 32 alphanumeric characters that identifies the SNMP view to be created. <*oid 32*> − The object ID that identifies an object tree (MIB tree) to be included or excluded from access by an SNMP manager. <*oid mask 32*> − The object mask ID that identifies an object tree (MIB tree) to be included or excluded from access by an SNMP manager. *view_type [included | excluded]* − Includes or excludes this object in the list of objects that an SNMP manager can access.

delete snmp view

The **delete snmp view** command removes an SNMP view previously created on the Switch.

delete snmp view	
Syntax	**delete snmp view <view_name 32> <oid 32>**
Parameter	<*view_name 32*> − A string of up to 32 alphanumeric characters that identifies the SNMP view to be deleted. <*oid 32*> − The object ID that identifies an object tree (MIB tree) that is deleted from the Switch.

show snmp view

The **show snmp view** command displays an SNMP view previously created on the Switch.

show snmp view	
Syntax	**show snmp view <view_name 32>**
Parameter	<*view_name 32*> − A string of up to 32 alphanumeric characters that identifies the SNMP view to be displayed.

create snmp community

The **create snmp community** command creates an SNMP community string and assigns access-limiting characteristics to this community string. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent.

An MIB view that defines the subset of all MIB objects to be accessible to the SNMP community.

Read/write or read-only level permission for the MIB objects accessible to the SNMP community.

create snmp community	
Syntax	**create snmp community <community_string 20> <username 32>**
Parameter	*<community_string 20>* − A string of up to 20 alphanumeric characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent. *<username 32>* − A string of up to 32 alphanumeric characters that identifies the SNMP community to be created.

delete snmp community

The **delete snmp community** command removes a previously defined SNMP community string from the Switch.

delete snmp community	
Syntax	**delete snmp community <community_string 32>**
Parameter	*<community_string 32>* − A string of up to 32 alphanumeric characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.

show snmp community

The **show snmp community** command displays SNMP community strings that are configured on the Switch.

show snmp community	
Syntax	**show snmp community <community_string 32>**
Parameter	*<community_string 32>* − A string of up to 32 alphanumeric characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.

config snmp engineID

The **config snmp engineID** command configures a name for the SNMP engine on the Switch.

config snmp engineID	
Syntax	**config snmp engineID <snmp_engineID 64>**
Parameter	*<snmp_engineID 64>* − A string up to 64 alphanumeric characters, to be used to identify the SNMP engine on the Switch.

show snmp engineID

The **show snmp engineID** command displays the identification of the SNMP engine on the Switch.

show snmp engineID	
Syntax	**show snmp engineID**
Parameter	None.

create snmp group

The **create snmp group** command creates a new SNMP group, or a table that maps SNMP users to SNMP views.

create snmp group	
Syntax	**create snmp group <groupname 32> [v1 | v2c | v3] {notify_view <view_name 32>} {read_view <view_name 32> | write_view <view_name 32>}**
Parameter	*<groupname 32>* − A name of up to 32 alphanumeric characters that identifies the SNMP group the new SNMP user is to be associated with. *v1* – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity − Ensures that packets have not been tampered with during transit. • Authentication − Determines if an SNMP message is from a valid source. • Encryption − Scrambles the contents of messages to prevent it from being viewed by an unauthorized source. *read_view* – Specifies that the SNMP group being created can request SNMP messages. • *<view_name 32*− A string of up to 32lphanumeric characters that identifies the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. *notify_view* − Specifies that the SNMP group being created can receive SNMP trap messages generated by the Switch's SNMP agent. • *<view_name 32*− A string of up to 32lphanumeric characters that identifies the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. *write_view* – Specifies that the SNMP group being created has write privileges. • *<view_name 32*− A string of up to 32lphanumeric characters that identifies the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.

delete snmp group

The **delete snmp group** command removes an SNMP group from the Switch.

delete snmp group	
Syntax	**delete snmp group <groupname 32>**
Parameter	*<groupname 32>* − A string of that identifies the SNMP group the new

SNMP user will be associated with. Up to 32 alphanumeric characters.

show snmp groups

The **show snmp groups** command displays the group-names of SNMP groups currently configured on the Switch. The security model, level, and status of each group are also displayed.

show snmp groups	
Syntax	**show snmp groups**
Parameter	None.

create snmp host

The **create snmp host** command creates a recipient of SNMP traps generated by the Switch's SNMP agent.

create snmp host	
Syntax	**create snmp host <ipaddr> [v1<username 32> | v2c<username 32> | v3 [noauth_nopriv | auth_nopriv | auth_priv]<username 32>]**
Parameter	*<ipaddr>* − The IP address of the remote management station to serve as the SNMP host for the Switch. *v1* – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity − ensures that packets have not been tampered with during transit. • Authentication − determines if an SNMP message is from a valid source. • Encryption − scrambles the contents of messages to prevent it being viewed by an unauthorized source. *<username 32>* − A string of up to 32 alphanumeric characters that identifies members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent. *noauth_nopriv* − Specifies that there is no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* − Specifies that authorization is required, but there is no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* − Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manger are encrypted

delete snmp host

The **delete snmp host** command deletes a recipient of SNMP traps generated by the Switch's SNMP agent.

delete snmp host

Syntax	**delete snmp host <ip_addr>**
Parameter	*<ip_addr>* − The IP address of a remote SNMP manager that receives SNMP traps generated by the Switch's SNMP agent. For example, 10.90.90.99.

show snmp host

The **show snmp host** command is used to display the IP addresses and configuration information of remote SNMP managers that are designated as recipients of SNMP traps generated by the Switch's SNMP agent.

show snmp host	
Syntax	**show snmp host <ip_addr>**
Parameter	*<ip_addr>* − The IP address of a remote SNMP manager that receives SNMP traps generated by the Switch's SNMP agent.

enable snmp traps

The **enable snmp traps** command enables SNMP trap support on the Switch.

enable snmp traps	
Syntax	**enable snmp traps**
Parameter	None.

disable snmp traps

The **disable snmp traps** command disables SNMP trap support on the Switch.

disable snmp traps	
Syntax	**disable snmp traps**
Parameter	None.

enable snmp authenticate traps

The **enable snmp authenticate traps** command enables SNMP authentication trap support on the Switch.

enable snmp authenticate traps	
Syntax	**enable snmp authenticate traps**
Parameter	None.

disable snmp authenticate traps

The **disable snmp authenticate traps** command disables SNMP authentication trap support on the Switch.

disable snmp authenticate traps	
Syntax	**disable snmp authenticate traps**
Parameter	None.

show snmp traps

The **show snmp traps** command displays the SNMP trap support status currently configured on the Switch.

show snmp traps	
Syntax	**show snmp traps**

Parameter	None.

enable snmp

The **enable snmp** command enables SNMP support on the Switch.

enable snmp	
Syntax	**enable snmp**
Parameter	None.

disable snmp

The **disable snmp** command disables SNMP support on the Switch.

disable snmp	
Syntax	**disable snmp**
Parameter	None.

enable snmp system_device_bootup traps

The **enable snmp system_device_bootup traps** command enables SNMP system device bootup traps support on the Switch. After enables the SNMP system device bootup traps support, the Switch will send out a trap to the SNMP manage host when the device is power on.

enable snmp system_device_bootup traps	
Syntax	**enable snmp system_device_bootup traps**
Parameter	None.

disable snmp system_device_bootup traps

The **disable snmp system_device_bootup traps** command disables SNMP system device bootup traps support on the Switch.

disable snmp system_device_bootup traps	
Syntax	**disable snmp system_device_bootup traps**
Parameter	None.

enable snmp fiber_port_link traps

The **enable snmp fiber_port_link traps** command enables SNMP fiber port link traps support on the Switch. After enables the SNMP fiber port link traps support, the Switch will send out a trap to the SNMP manage host when the fiber port is link up or link down.

enable snmp fiber_port_link traps	
Syntax	**enable snmp fiber_port_link traps**
Parameter	None.

disable snmp fiber_port_link traps

The **disable snmp fiber_port_link traps** command disables SNMP fiber port link traps support on the Switch.

disable snmp fiber_port_link traps	
Syntax	**disable snmp fiber_port_link traps**
Parameter	None.

enable snmp firmware_upgrade_state traps

The **enable snmp firmware_upgrade_state traps** command enables SNMP firmware upgrade state traps support on the Switch. After enables the SNMP firmware upgrade state traps support, the Switch will send out a trap to the SNMP manage host when the firmware upgrade is succeed or fail.

enable snmp firmware_upgrade_state traps	
Syntax	**enable snmp firmware_upgrade_state traps**
Parameter	None.

disable snmp firmware_upgrade_state traps

The **disable snmp firmware_upgrade_state traps** command disable SNMP firmware upgrade state traps support on the Switch.

disable snmp firmware_upgrade_state traps	
Syntax	**disable snmp firmware_upgrade_state traps**
Parameter	None.

enable snmp rstpport_state_change traps

The **enable snmp rstpport_state_change traps** command enables SNMP rstp port state change traps support on the Switch. After enables the SNMP RSTP port state change traps support, the Switch will send out a trap when the state of RSTP port is changed.

enable snmp rstpport_state_change traps	
Syntax	**enable snmp rstpport_state_change traps**
Parameter	None.

disable snmp rstpport_state_change traps

The **disable snmp rstpport_state_change traps** command disables SNMP rstp port state change traps support on the Switch.

disable snmp rstpport_state_change traps	
Syntax	**disable snmp rstpport_state_change traps**
Parameter	None.

8 DOWNLOAD/UPLOAD Commands

The Download/Upload commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
download	[configuration <ip_addr> <path_filename 64> startup | firmware <ip_addr> <string 64> | ssl certificate <ip_addr> certfilename <path_filename 64>]
upload	[firmware <ip_addr> <path_filename 64> | cfg_toTFTP <ip_addr> <path_filename 64> config_id <value 1-2>]
config dhcp_server screening	ports <portlist> state [enable | disable]
show dhcp_server screening	
config filter dhcp_server	[add | delete] permit server_ip <ipaddr> [client_mac <macaddr> | ports <portlist>]

Each command is listed in detail, as follows:

download

The **download** command downloads a configuration, firmware or ssl file from a TFTP server.

download	
Syntax	**download [configuration <ip_addr> <path_filename 64> startup | firmware <ip_addr> <string 64> | ssl certificate <ip_addr> certfilename <path_filename 64>]**
Parameter	*configuration* − Downloads a switch configuration file from a TFTP server. *<ip_addr>* − The IP address of the TFTP server. For example, 10.1.2.3/255.0.0.0. *<path_filename 64>* − The DOS path and filename of the firmware or switch configuration file, up to 64 characters, on the TFTP server. For example, C:\31xx.had. *startup* − Indicates the Configuration file is to be downloaded to the startup config. *firmware* − Downloads and installs firmware on the Switch from a TFTP server. *<string 64>* − The DOS path and filename of the firmware file, up to 64 characters, on the TFTP server. For example, C:\31xx.had. *ssl* − Downloads ssl file from a TFTP server.

Note: Switch will reboot after restore and all current configurations will be lost

upload

The **upload** command uploads the Switch's current settings or firmware to a TFTP server.

upload	
Syntax	**upload [firmware <ip_addr> <path_filename 64> | cfg_toTFTP <ip_addr> <path_filename 64> config_id <value 1-2>]**
Parameter	*firmware* − Uploads and installs firmware to a TFTP server from the

switch.

cfg_toTFTP − Uploads a switch configuration file to a TFTP server from the switch.

ssl − Uploads ssl file from a TFTP server.

<*ip_addr*> − The IP address of the TFTP server.

<*path_filename 64*> − The DOS path and filename of the firmware or switch configuration file, up to 64 characters, on the TFTP server. For example, C:\31xx.had.

config_id <*value 1-2*> − Specify to upload configuration file 1 or 2.

config dhcp_server screening

The **config dhcp_server screening** command configure the DHCP server screening of the switch.

config dhcp_server screening	
Syntax	**config dhcp_server screening ports <portlist> state [enable | disable]**
Parameter	<*portlist*> − A port or range of ports to be configured. *state [enable* | *disable]* − Enables or disables the DHCP server screening for the switch.

show dhcp_server screening

The **show dhcp_server screening** command displays the DHCP server screening of the switch.

show dhcp_server screening	
Syntax	**show dhcp_server screening**
Parameter	None.

config filter dhcp_server

The **config filter dhcp_server** command specifies the system image that the device loads at startup, or the specific image that is to be deleted.

config filter dhcp_server	
Syntax	**config filter dhcp_server [add | delete] permit server_ip <ipaddr> [client_mac <macaddr> | ports <portlist>]**
Parameter	*[add* | *delete]* − Add or delete the specific permit server IP for the config filter DHCP server on the switch. <*ipaddr*> − The IP address of the DHCP filter server. <*macaddr*> − The MAC address of the DHCP filter server. <*portlist*> − A port or range of ports to be configured.

9 DHCP Local Relay Commands

The DHCP local relay commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config dhcp_local_relay vlan	<vlan_name> state [enable | disable]

Each command is listed in detail, as follows:

config dhcp _local_relay vlan

Each VLAN which was added to the DHCP Local Relay list participates in the DHCP Local Relay process – Option 82 is added to DHCP requests on this VLAN, and Removed from DHCP Replies on this VLAN.

config dhcp_local_relay vlan	
Syntax	**config dhcp_local_relay vlan <vlan_name> state [enable | disable]**
Parameter	<*vlan_name*> – The VLAN name identifier. *state* – Enables or disables the DHCP local relay VLAN status.

10 *NETWORK MONITORING Commands*

The Network Monitoring commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
show packet ports	<portlist>
show error ports	<portlist>
show utilization	[ports | cpu | mem]
clear counters	
clear log	
show log	
enable syslog	
disable syslog	
show syslog	
create syslog host	<index 1-4> ipaddress <ipaddr> {severity [informational | warning | all] | facility [local0 | local1| local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number 1-65535> | state[enable | disable]}
config syslog host	[all | <index 1-4>] {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state[enable | disable]}
delete syslog host	[<index 1-4> | all]
show syslog host	{<index 1-4>}
cable diagnostic	port [portlist | all]

Each command is listed in detail, as follows:

show packet ports

The **show packet ports** command displays statistics about packets sent and received by ports specified in the port list.

show packet ports	
Syntax	**show packet ports <portlist>**
Parameter	*<portlist>* − A port or range of ports whose statistics are to be displayed.

show error ports

The **show error ports** command displays all of the packet error statistics collected and logged by the Switch for a given port list.

show error ports	
Syntax	**show error ports <portlist>**
Parameter	*<portlist>* − A port or range of ports whose error statistics are to be displayed.

show utilization

The **show utilization** command displays the real-time utilization statistics for ports in bits per second (bps) for the Switch, and for the CPU in percentage.

show utilization	
Syntax	**show utilization [ports | cpu | mem]**
Parameter	None.

clear counters

The **clear counters** command clears the counters used by the Switch to compile statistics.

clear counters	
Syntax	**clear counters**
Parameter	None.

clear log

The **clear log** command clears the Switch's history log.

clear log	
Syntax	**clear log**
Parameter	None.

show log

The **show log** command displays the contents of the Switch's history log.

show log	
Syntax	**show log**
Parameter	None.

enable syslog

The **enable syslog** command enables the system log to be sent to a remote host.

enable syslog	
Syntax	**enable syslog**
Parameter	None.

disable syslog

The **disable syslog** command disables the system log to be sent to a remote host.

disable syslog	
Syntax	**disable syslog**
Parameter	None.

show syslog

The **show syslog** command displays the syslog status (enabled or disabled).

show syslog	
Syntax	**show syslog**
Parameter	None.

create syslog host

The **create syslog host** command creates a new syslog host.

create syslog host

Syntax **create syslog host <index 1-4> ipaddress <ipaddr> {severity [informational | warning | all] | facility [local0 | local1| local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number 1-65535> | state[enable | disable]}**

Parameter *<index 1-4>* − The syslog host index id. There are four available indices, numbered 1 to 4.

ipaddress <ipaddr> − The IP address of the remote host to which syslog messages are to be sent. For example, 10.90.90.99.

severity − The message severity level indicator. These are described in the table below (Bold font indicates that the corresponding severity level is currently supported on the Switch):

Numerical Code	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

informational − Specifies that informational messages are to be sent to the remote host. This corresponds to number 6 from the list above.

warning − Specifies that warning messages are to be sent to the remote host. This corresponds to number 4 from the list above.

all − Specifies that all of the currently supported syslog messages that are generated by the Switch are to be sent to the remote host.

facility − Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the 'local use' facilities or they may use the 'user-level' Facility. Those Facilities that have been designated are shown in the table below (Bold font indicates the facility values that the Switch currently supports):

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslog
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert

15	clock daemon
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

local0 − Specifies that local use 0 messages are to be sent to the remote host. This corresponds to number 16 from the list above.

local1 − Specifies that local use 1 messages are to be sent to the remote host. This corresponds to number 17 from the list above.

local2 − Specifies that local use 2 messages are to be sent to the remote host. This corresponds to number 18 from the list above.

local3 − Specifies that local use 3 messages are to be sent to the remote host. This corresponds to number 19 from the list above.

local4 − Specifies that local use 4 messages are to be sent to the remote host. This corresponds to number 20 from the list above.

local5 − Specifies that local use 5 messages are to be sent to the remote host. This corresponds to number 21 from the list above.

local6 − Specifies that local use 6 messages are to be sent to the remote host. This corresponds to number 22 from the list above.

local7 − Specifies that local use 7 messages is sent to the remote host. This corresponds to number 23 from the list above.

udp_port <udp_port_number 1-65535> − Specifies the UDP port number that the syslog protocol is to use to send messages to the remote host.

state [enable | disable] − Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.

config syslog host

The **config syslog host** command configures the syslog protocol to send system log information to a remote host.

config syslog host	
Syntax	**config syslog host [all | <index 1-4>] {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state[enable | disable]}**
Parameter	*all* − Specifies that the command is to be applied to all hosts. *<index 1-4>* − The syslog host index id. There are four available indices, numbered 1 to 4. *ipaddress <ipaddr>* − The IP address of the remote host to which syslog messages are to be sent. *severity* − The message severity level indicator. These are described in the table below (Bold font indicates that the corresponding severity level is currently supported on the Switch): Numerical Code — Severity 0 — Emergency: system is unusable

1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

informational − Specifies that informational messages are to be sent to the remote host. This corresponds to number 6 from the list above.

warning − Specifies that warning messages are to be sent to the remote host. This corresponds to number 4 from the list above.

all − Specifies that all of the currently supported syslog messages that are generated by the Switch are to be sent to the remote host.

facility − Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the 'local use' facilities or they may use the 'user-level' Facility. Those Facilities that have been designated are shown in the table below (Bold font indicates the facility values that the Switch currently supports):

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslog
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

local0 − Specifies that local use 0 messages are to be sent to the remote host. This corresponds to number 16 from the list above.

local1 − Specifies that local use 1 messages are to be sent to the remote host. This corresponds to number 17 from the list above.

local2 − Specifies that local use 2 messages are to be sent to the remote host. This corresponds to number 18 from the list above.

local3 − Specifies that local use 3 messages are to be sent to the remote host. This corresponds to number 19 from the list above.

local4 − Specifies that local use 4 messages are to be sent to the remote host. This corresponds to number 20 from the list above.

local5 − Specifies that local use 5 messages are to be sent to the remote host. This corresponds to number 21 from the list above.

local6 − Specifies that local use 6 messages are to be sent to the remote host. This corresponds to number 22 from the list above.

local7 − Specifies that local use 7 messages is sent to the remote host. This corresponds to number 23 from the list above.

udp_port <udp_port_number 1-65535> − Specifies the UDP port number that the syslog protocol is to use to send messages to the remote host.

ipaddress <ipaddr> − Specifies the IP address of the remote host to which syslog messages are to be sent.

state [enable | disable] − Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.

delete syslog host

The **delete syslog host** command removes a previously configured syslog host from the Switch.

delete syslog host	
Syntax	**delete syslog host [<index 1-4> | all]**
Parameter	*<index 1-4>* − The syslog host index id. There are four available indices, numbered 1 to 4. *all* − Specifies that the command applies to all hosts.

show syslog host

The **show syslog host** command displays the syslog hosts that are currently configured on the Switch.

show syslog host	
Syntax	**show syslog host {<index 1-4>}**
Parameter	*<index 1-4>* − The syslog host index id. There are four available indices, numbered 1 to 4.

cable diagnostic

The **cable diagnostic** command is used to determine if there are any errors on the copper cables and the position where the errors may have occurred.

cable diagnostic	
Syntax	**cable diagnostic port [portlist | all]**
Parameter	*<portlist>* – A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured.

11 MAC Notification Commands

The MAC Notification commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table

Command	Parameter
enable mac_notification	
disable mac_notification	
config mac_notification	{[historysize <int 1-500>] | [interval <int 1-2147483647>]}
config mac_notification ports	[<portlist> | all] [enable | disable]
show mac_notification	
show mac_notification ports	<portlist>

Each command is listed in detail, as follows:

enable mac_notification

The **enable mac_notification** command enables the MAC notification globally on the Switch.

enable mac_notification	
Syntax	**enable mac_notification**
Parameter	None.

disable mac_notification

The **disable mac_notification** command disables the MAC notification globally on the Switch.

disable mac_notification	
Syntax	**disable mac_notification**
Parameter	None.

config mac_notification

The **config mac_notification** is used to monitor MAC addresses which learned and entered into the forwarding database.

config mac_notification	
Syntax	**config mac_notification {[historysize <int 1-500>] | [interval <int 1-2147483647>]}**
Parameter	*historysize <int 1-500>* - Specify the maximum number of entries listed in the history log used for notification. The range is between 1 and 500. *interval <int 1-2147483647>* - Specify the time interval between notification. The range is between 1 and 2147483647 seconds.

config mac_notification ports

The **config mac_notification ports** is used to monitor MAC addresses which learned and entered into the forwarding database.

config mac_notification ports	
Syntax	**config mac_notification ports [<portlist> | all] [enable | disable]**
Parameter	*<portlist>* - Specify a port or range of ports to be configured. *all* – Specify all ports to be configured.

[enable | disable] – Specify the MAC address table notification to be enabled or disabled on the Switch.

show mac_notification

The **show mac_notification** is used to display the Switch's MAC address table notification global settings.

show mac_notification	
Syntax	**show mac_notification**
Parameter	None.

show mac_notification ports

The **show mac_notification ports** is used to display the Switch's MAC address table notification status settings.

show mac_notification ports	
Syntax	**show mac_notification ports <portlist>**
Parameter	*<portlist>* - Specify a port or range of ports to be displayed.

12 *SPANNING TREE Commands*

The Spanning tree commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table

Command	Parameter
config stp	{maxage <value 6-40> | hellotime <value 1-10> | mst_config_id [name <string 32> | mst_ports <portlist> | priority <value 0-61440>| txholdcount <value 1-10> | forwarddelay <value 4-30>| fbpdu [enable | disable]}
config stp ports	<portlist> {externalcost [auto | <value 1-200000000>] | edge [auto | true | false] | p2p [true | false | auto] | state [enable | disable] | migrate [no | yes] | fbpdu [enable | disable] | priority <value 0-240> | restricted_role [true | false] | restricted_tcn [true | false] }
config stp version	[mstp | rstp | stp]
enable stp	
disable stp	
show stp	
show stp ports	<portlist>
show stp instance	{<value 0-15>}
show stp mst_config_id	
config stp priority	<value 0-61440> instance_id <value 0-15>
config stp mst_config_id	[revision_level <int 0-65535> | name <string 32>]
config stp mst_ports	<portlist> instance_id <value 0-15> {internalCost [auto | value 1-200000000] | priority <value 0-240>}

Each command is listed in detail, as follows:

config stp

The **config stp** command configures the Spanning Tree Protocol (STP) for the entire switch. All commands here are implemented for the STP version that is currently set on the Switch.

config stp	
Syntax	**config stp {maxage <value 6-40> | hellotime <value 1-10> | mst_config_id [name <string 32> | mst_ports <portlist> | priority <value 0-61440>| txholdcount <value 1-10> | forwarddelay <value 4-30>| fbpdu [enable | disable]}**
Parameter	*maxage* <*value 6-40*> − This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value aids in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch starts sending its own BPDU to all other switches for permission to become the Root Bridge. If your switch has the lowest priority, it becomes the Root Bridge. The user may choose a time between 6 and 40 seconds. The default value is 20. *hellotime* <*value 1-10*> − The user may set the time interval between transmission of configuration messages by the root device in STP, or by the designated router, thus stating that the Switch is still functioning. The value may be between 1 and 10 seconds. The default value is 2 seconds.

name <*string 32*> − Specifies the stp name.

<*portlist*> – A port or range of ports to be configured.

priority <*value 0-61440*> − Specifies the stp priority for the ports of switch. The range is between 0 and 61440.

txholdcount <*value 1-10*> − Specifies the TX hold counter for the ports of Switch. The range is between 1 and 10.

forwarddelay <*value 4-30*> − The amount of time (in seconds) that the root device will wait before changing from Blocking to Listening , and from Listening to Learning states. The value may be between 4 and 30 seconds. The default is 15 seconds.

fbpdu [enable | *disable]* − Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is disabled.

config stp ports

The **config stp ports** command configures STP for a group of ports.

config stp ports	
Syntax	**config stp ports <portlist> {externalcost [auto | <value 1-200000000>] | edge [auto | true | false] | p2p [true | false | auto] | state [enable | disable] | migrate [no | yes] | fbpdu [enable | disable] | priority <value 0-240> | restricted_role [true | false] | restricted_tcn [true | false] }**
Parameter	<*portlist*> – A port or range of ports to be configured. The port list is specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified. The beginning and end of the port list range are separated by a dash. *externalcost* − Defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is auto. • *auto* – Automatically sets the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost:10Mbps port = 2000000. 100Mbps port = 200000. Gigabit port = 20000. Port-channel = 20000. • <*value 1-200000000*> - Defines a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. *edge [true*	*false] – true* designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. *false* indicates that the port does not have edge port status. The default setting for this parameter is false. *p2p [true*	*false*	*auto] – true* indicates a point-to-point (P2P) link. P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of *false* indicates that the port cannot have p2p status. *auto* allows the port to have p2p status whenever possible and operate as if the p2p status were true. (A port that operates in full-duplex is assumed to be point-to-point, while a half-duplex port is considered as a shared port). If the port cannot maintain this status (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were *false*. The default setting for this parameter is *auto*. *state [enable*	*disable]* − Allows STP to be enabled or disabled for the ports specified in the port list. The default is enabled.

migrate [no | yes] − Allows STP to be enabled or disabled for the ports specified in the port list. The default is no.

fbpdu [enable | disable | system] − If enabled - allows the forwarding of STP BPDU packets from other network devices Disable – blocking STP BPDU packets from other network devices. System – indicates that port will behave as global switch's fbpdu value configured. Fbpdu value valid only when STP port state is disabled or global STP state is disabled. The default is system.

priority <value 0-240> − Specifies the priority for the port interface. The value may be between 0 and 240. A lower number denotes a higher priority. A higher priority designates the interface to forward packets first.

restricted_role [true | false] − Specifies the restricted role status in the port list. The default is false.

restricted_tcn [true | false] − Specifies the restricted tcn status in the port list. The default is false.

config stp version

The **config stp version** command sets the version of the spanning tree to be implemented on the Switch.

config stp version	
Syntax	**config stp version [mstp | rstp | stp]**
Parameter	*mstp* – Sets the Multiple Spanning Tree Protocol (MSTP) globally on the Switch. *rstp* – Sets the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. *stp* – Sets the Spanning Tree Protocol (STP) globally on the Switch.

enable stp

The **enable stp** command sets the Spanning Tree Protocol to be globally enabled on the Switch.

enable stp	
Syntax	**enable stp**
Parameter	None.

disable stp

The **disable stp** command sets the Spanning Tree Protocol to be globally disabled on the Switch.

disable stp	
Syntax	**disable stp**
Parameter	None.

show stp

The **show stp** command displays the Switch's current STP configuration.

show stp	
Syntax	**show stp**
Parameter	None.

show stp ports

The **show stp ports** command displays the STP Instance Settings and STP Instance Operational Status currently implemented on the Switch.

show stp ports	
Syntax	**show stp ports <portlist>**
Parameter	*<portlist>* – A port or range of ports to be configured. The port list is specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified.

show stp instance

The **show stp instance** command displays the Switch's current STP Instance Settings and the STP Instance Operational Status.

show stp instance	
Syntax	**show stp instance {<value 0-15>}**
Parameter	*<value 0-15>* - The value of the previously configured instance on the Switch. The value may be between 0 and 15. An entry of 0 displays the STP configuration for the CIST internally set on the Switch.

show stp mst_config_id

The **show stp mst_config_id** command displays the Switch's current MSTP configuration identification.

show stp mst_config_id	
Syntax	**show stp mst_config_id**
Parameter	None.

config stp priority

The **config stp priority** command updates the STP instance configuration settings on the Switch. The MSTP uses the priority in selecting the root bridge, root port and designated port. Assigning higher priorities to STP regions instructs the Switch to give precedence to the selected instance_id for forwarding packets. A lower value indicates a higher priority.

config stp priority	
Syntax	**config stp priority <value 0-61440> instance_id <value 0-15>**
Parameter	*priority <value 0-61440>* - The priority for a specified *instance_id* for forwarding packets. The value may be between 0 and 61440, and must be divisible by 4096. A lower value indicates a higher priority. *instance_id <value 0-15>* - The value of the previously configured instance id for which the user wishes to set the priority value. An instance_id of 0 denotes the default instance_id (CIST) internally set on the Switch.

config stp mst_config_id

The **config stp mst_config_id** command uniquely identifies the MSTP configuration currently configured on the Switch. Information entered here is attached to BDPU packets as an identifier for the MSTP region to which it belongs. Switches having the same revision_level, name and identical vlans mapped for STP instance_ids are considered to be part of the same MSTP region.

config stp mst_config_id	
Syntax	**config stp mst_config_id [revision_level <int 0-65535> | name <string 32>]**
Parameter	*revision_level <int 0-65535>*– The MSTP configuration revision number. The value may be between 0 and 65535. This value, along with the name and identical vlans mapped for STP instance_ids identifies the MSTP region configured on the Switch. The default setting

is 0.

name <*string 32*> - A string of up to 32 alphanumeric characters to uniquely identify the MSTP region on the Switch. This name, along with the revision_level value and identical vlans mapped for STP instance_ids identifies the MSTP region configured on the Switch. If no name is entered, the default name is the MAC address of the device.

config stp mst_ports

The **config stp mst_config_id** command uniquely identifies the MSTP configuration currently configured on the Switch. Information entered here is attached to BDPU packets as an identifier for the MSTP region to which it belongs. Switches having the same revision_level, name and identical vlans mapped for STP instance_ids are considered to be part of the same MSTP region.

config stp mst_ports	
Syntax	**config stp mst_ports <portlist> instance_id <value 0-15> {internalCost [auto | value 1-200000000] | priority <value 0-240>}**
Parameter	*<portlist>* – A port or range of ports to be configured. The port list is specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified. The beginning and end of the port list range are separated by a dash. For example, type 1-4 to specifies the port 1 to port 4. *instance_id* <*value 0-15*> - The value may be between 0 and 15. An entry of 0 denotes the CIST (Common and Internal Spanning Tree. *internalCost* – The relative cost of forwarding packets to specified ports when an interface is selected within an STP instance. The default setting is auto. There are two options: • *auto* – Specifies setting the quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. • *value 1-200000000* – Specifies setting the quickest route when a loop occurs. The value may be in the range of 1-200000000. A lower internalCost represents a quicker transmission. *priority* <*value 0-240*> - The priority for the port interface The value may be between 0 and 240. A lower number denotes a higher priority. A higher priority designates the interface to forward packets first.

13 *FORWARDING DATABASE Commands*

The Forwarding Database commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create fdb	<vlan_name 32> <macaddr> port <port 1-*maxport*>
create multicast_fdb	<integer 1-4094> <macaddr>
config multicast_fdb	<integer 1-4094> <macaddr> [add | delete] <portlist>
config fdb aging_time	<sec 10-600>
delete fdb	<vlan_name 32> <macaddr>
clear flood_fdb	
show multicast_fdb	{vlan <vlan_name 32> | mac_address <macaddr>}
show fdb	{port <port 1-*maxport*> | vlan <vlan_name 32> | vlanid <vidlist> | mac_address <macaddr> | static | aging_time}
config multicast_filtering_mode	[vlan <vlan_name 32>] [forward_unregistered_groups | filter_unregistered_groups]
show multicast_filtering_mode	{vlan <vlan_name 32>}

Each command is listed in detail, as follows:

create fdb

The **create fdb** command creates a static entry in the Switch's unicast MAC address forwarding database.

create fdb	
Syntax	**create fdb <vlan_name 32> <macaddr> port <port 1-*maxport*>**
Parameter	*<vlan_name 32>* − The name of the VLAN on which the MAC address resides. *<macaddr>* − The MAC address to be added to the forwarding table. For example, 01:00:5E:00:00:00. *port <port 1-maxport>* − The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.

Note: The syntax maxport for DES-1210-10 is 10 and 28 for DES-1210-38.

create multicast_fdb

The **create multicast_fdb** command creates a static entry in the multicast MAC address forwarding table (database).

create fdb	
Syntax	**create multicast_fdb <integer 1-4094> <macaddr>**
Parameter	*<integer 1-4094>* − The item of the VLAN on which the MAC address resides. The range is between 1 and 4094. *<macaddr>* − The MAC address to be added to the forwarding table.

config multicast_fdb

The **config multicast_fdb** command configures the multicast MAC address forwarding table.

config multicast_fdb	
Syntax	**config multicast_fdb <integer 1-4094> <macaddr> [add | delete] <portlist>**
Parameter	*<integer 1-4094>* − The item of the VLAN on which the MAC address resides. The range is between 1 and 4094. *<macaddr>* − The MAC address to be configured to the forwarding table. *add* − Specifies that the MAC address is to be added to the forwarding table. Delete will remove the MAC address from the forwarding table. *delete* − Specifies that the MAC address is to be removed from the forwarding table. *<portlist>* − A port or range of ports to be configured.

config fdb aging_time

The **config fdb aging_time** command sets the aging time of the forwarding database. The aging time affects the learning process of the Switch. Dynamic forwarding table entries, which are made up of the source MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time. The aging time can be from 0 to 600 seconds with a default value of 5 minutes. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the Switch. If the aging time is too short however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the Switch will broadcast the packet to all ports, negating many of the benefits of having a Switch.

config fdb aging_time	
Syntax	**config fdb aging_time <sec 10-600>**
Parameter	*<sec 0-600>* − The aging time for the MAC address forwarding database value, in seconds.

delete fdb

The **delete fdb** command deletes an entry in the Switch's MAC address forwarding database.

delete fdb	
Syntax	**delete fdb <vlan_name 32> <macaddr>**
Parameter	*<vlan_name 32>* − The name of the VLAN on which the MAC address resides. *<macaddr>* − The MAC address to be removed from the forwarding table.

clear flood_fdb

The **clear flood_fdb** command clears dynamically learned entries from the Switch's forwarding database.

clear flood_fdb	
Syntax	**clear flood_fdb**
Parameter	None.

show multicast_fdb

The **show multicast_fdb** command displays the current contents of the Switch's multicast MAC address forwarding database.

show multicast_fdb	
Syntax	**show multicast_fdb {vlan <vlan_name 32> | mac_address <macaddr>}**
Parameter	*vlan <vlan_name 32>* − The name of the VLAN on which the MAC address resides. *mac_address <macaddr>* − The MAC address that will be added to the forwarding table.

show fdb

The **show fdb** command displays the current contents of the Switch's forwarding database.

show fdb	
Syntax	**show fdb {port <port 1-*maxport*> | vlan <vlan_name 32> | vlanid <vidlist> | mac_address <macaddr> | static | aging_time}**
Parameter	*<port 1-maxport>* − The port number corresponding to the MAC destination address. The Switch always forwards traffic to the specified device through this port. *<vlan_name 32>* − The name of the VLAN on which the MAC address resides. *<vidlist>* − The vid of the VLAN on which the MAC address resides. *<macaddr>* − The MAC address entry in the forwarding table. *static* − Specifies that static MAC address entries are to be displayed. *aging_time* − Displays the aging time for the MAC address forwarding database.

Note: The syntax maxport for DES-1210-10 is 10 and 28 for DES-1210-38.

config multicast_filtering_mode

The **config multicast_filtering_mode** command enables filtering of multicast addresses.

config multicast_filtering_mode	
Syntax	**config multicast_filtering_mode [vlan <vlan_name 32>] [forward_unregistered_groups | filter_unregistered_groups]**
Parameter	*<vlan_name 32>* − The name of the VLAN on which the MAC address resides. *forward_unregistered_groups* - Forwards unregistered multicast packets. *filter_unregistered_groups* - Filter unregistered multicast packets.

show multicast_filtering_mode

The **show multicast_filtering_mode** command displays the filtering of multicast addresses.

show multicast_filtering_mode	
Syntax	**show multicast_filtering_mode {vlan <vlan_name 32>}**
Parameter	*<vlan_name 32>* − The name of the VLAN on which the MAC address resides.

14 BROADCAST STORM CONTROL Commands

The Broadcast Storm Control commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config traffic control	{<portlist> | all} [broadcast {enable | disable}] [multicast {enable | disable}] [unicast {enable | disable}] [threshold <value 0-1024000>]
show traffic control	{<portlist>}

Each command is listed in detail, as follows:

config traffic control

The **config traffic control** command configures broadcast, multicast and unknown unicast storm control.

config traffic control	
Syntax	**config traffic control {<portlist> | all} [broadcast {enable | disable}] [multicast {enable | disable}] [unicast {enable | disable}] [threshold <value 0-1024000>]**
Parameter	*<portlist>* - A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured. *broadcast* – Enables broadcast storm control only. *multicast* – Enables multicast storm control only. *unicast* – Enables unicast storm control only. *threshold <value 0-1024000>* − The upper threshold at which the specified traffic control is switched on. The value is the number of broadcast/multicast/unicast packets, in Kbps, received by the Switch that will trigger the storm traffic control measures. The value ranges in size from 0 to 1024000 Kbps.

show traffic control

The **show traffic control** command displays the current storm traffic control configuration on the Switch.

show traffic control	
Syntax	**show traffic control {<portlist>}**
Parameter	*<portlist>* - A port or range of ports whose settings are to be displayed.

15 QOS Commands

The QoS commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config scheduling	<class_id 0-3> weight <value 1-55>
show scheduling	
config bandwidth_control	[<portlist> | all] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit | <value 64-1024000>]}
show bandwidth_control	[<portlist> | all]
config cos port_mapping	class <class_id 0-3> port [<portlist> | all]
show cos port_mapping	{port <portlist>}
config cos mapping	port [<portlist> | all] [802.1p | dscp | none | port_mapping]
show cos mapping	{port <portlist>
config cos mac_mapping	destination_addr <macaddr> class <class_id 0-3>
show cos mac_mapping	{destination_addr <macaddr>}
delete cos mac_mapping	destination_addr <macaddr>
config cos ip_mapping	destination_ip <ipaddr> class <class_id 0-3>
show cos ip_mapping	{destination_ip <ipaddr>}
delete cos ip_mapping	destination_ip <ipaddr>
config cos tcp_port_mapping	destination_port <value 0-65535> class <class_id 0-3>
show cos tcp_port_mapping	{destination_port <value 0-65535>}
delete cos tcp_port_mapping	destination_port <value 0-65535>
config cos udp_port_mapping	destination_port <value 0-65535> class <class_id 0-3>
show cos udp_port_mapping	{destination_port <value 0-65535>}
delete cos udp_port_mapping	destination_port <value 0-65535>
config cos vlanid_mapping	vid <vlanid 1-4094> class <class_id 0-3>
show cos vlanid_mapping	{vid <vlanid 1-4094>}
delete cos vlanid_mapping	vid <vlanid 1-4094>
config cos protocol_mapping	protocol <ip_protocol 1-255> class <class_id 0-3>
show cos protocol_mapping	{protocol <ip_protocol 1-255>}
delete cos protocol_mapping	protocol <ip_protocol 1-255>
config 802.1p user_priority	<priority 0-7> <class_id 0-3>
show 802.1p user_priority	

config 802.1p default_priority	[<portlist> | all] <priority 0-7>
show 802.1p default_priority	
config scheduling_mechanism	[strict | wrr]
show scheduling_mechanism	
config dscp_mapping	dscp_value <value 0-63> class <class_id 0-3>]
show dscp_mapping	{dscp_value <value 0-63>}

Each command is listed in detail, as follows:

config scheduling

The **config scheduling** command configures traffic scheduling for each of the Switch's QoS queues.

The Switch contains four hardware classes of service. Incoming packets must be mapped to one of these four hardware queues. This command is used to specify the rotation by which these four hardware queues are emptied.

The Switch's default (if the **config scheduling** command is not used) is to empty the hardware queues in order – from the highest priority queue (hardware class 3) to the lowest priority queue (hardware class 0). Each hardware queue transmits all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue can again transmit any packets it may have received.

The max_packets parameter allows the user to specify the maximum number of packets a given hardware priority queue can transmit before allowing the next lowest hardware priority queue to begin transmitting its packets. A value between 0 and 15 can be specified. For example, if a value of 3 is specified for all the queues, then the highest hardware priority queue (number 3) will be allowed to transmit 3 packets – then the next lowest hardware priority queue (number 2) will be allowed to transmit 3 packets, and so on, until all of the queues have transmitted 3 packets. The process will then repeat.

config scheduling	
Syntax	**config scheduling <class_id 0-3> weight <value 1-55>**
Parameter	*<class_id 0-3>* − The hardware classes of service to which the config scheduling command is to be applied. The four hardware classes of service are identified by number (from 0 to 3) with class 3 having the highest priority. *weight <value 1-55>* − Specifies the maximum number of packets the above specified priority class of service is allowed to transmit before allowing the next lower priority class of service to transmit its packets. The value may be between 1 and 55 packets.

show scheduling

The **show scheduling** command displays the current configuration for the maximum number of packets (*weightt*) value assigned to the four priority classes of service on the Switch. The Switch empties the four hardware queues in order, from the highest priority (class 3) to the lowest priority (class 0).

show scheduling	
Syntax	**show scheduling**
Parameter	None.

config bandwidth_control

The **config bandwidth_control** command defines bandwidth control.

config bandwidth_control	
Syntax	**config bandwidth_control [<portlist> | all] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit | <value 64-1024000>]}**
Parameter	*<portlist>* - A port or range of ports to be configured. *all* - Specifies that the **config bandwidth_control** command applies to all ports on the Switch. *rx_rate* - Enables ingress rate limiting • *no_limit* – Indicates no limit is defined. • <*value 64–1024000*>] – Indicates a range between 64-*1024000*kbps. *tx_rate* – Enables egress rate limiting. • *no_limit* – Indicates no limit is defined. • <value *64-1024000>]* – Indicates a range between 64-*1024000*kbps*.*

show bandwidth_control

The **show bandwidth_control** command displays bandwidth control.

show bandwidth_control	
Syntax	**show bandwidth_control [<portlist> | all]**
Parameter	*<portlist>* - A port or range of ports to be configured. *all* - Specifies that the **show bandwidth_control** command applies to all ports on the Switch.

config cos port_mapping

The **config cos port_mapping** command is used to configure the CoS port mapping method on the Switch.

config cos port_mapping	
Syntax	**config cos port_mapping class <class_id 0-3> port [<portlist> | all]**
Parameter	*class<class_id 0-3>* - Specifies the number of the Switch's hardware priority queue. *<portlist>* - A port or range of ports to be configured. *all* - Specifies all ports to be configured on the Switch.

show cos port_mapping

The **show cos port_mapping** command displays the CoS port mapping on the Switch.

show cos port_mapping	
Syntax	**show cos port_mapping {port <portlist>}**
Parameter	*<portlist>* - A port or range of ports to be displayed.

config cos mapping

The **config cos mapping** command is used to configure the method of which incoming packets will be identified for the CoS to port mapping feature on the Switch.

config cos mapping	
Syntax	**config cos mapping port [<portlist> | all] [802.1p | dscp | none | port_mapping]**

Parameter	*<portlist>* - A port or range of ports to be configured. *all* - Specifies all ports to be configured on the Switch. *[802.1p | dscp | none | port_mapping]* – Specified which incoming packets will be identified for the CoS.

show cos mapping

The **show cos mapping** command displays the information regarding CoS mapping enabled ports and their mapping method.

show cos mapping	
Syntax	**show cos mapping {port <portlist>}**
Parameter	*<portlist>* - A port or range of ports to be displayed.

config cos mac_mapping

The **config cos mac_mapping** command is used to configure the CoS MAC mapping method on the Switch.

config cos mac_mapping	
Syntax	**config cos mac_mapping destination_addr <macaddr> class <class_id 0-3>**
Parameter	*<macaddr>* - Specifies the MAC address to be mapped. For example, 01:00:5E:00:00:00. *<class_id 0-3>* - Specifies the number of the Switch's hardware priority queue.

show cos mac_mapping

The **show cos mac_mapping** command is displays the information regarding CoS MAC mapping enabled ports and their mapping method.

show cos mac_mapping	
Syntax	**show cos mac_mapping {destination_addr <macaddr>}**
Parameter	*<macaddr>* - The MAC address to be displayed..

delete cos mac_mapping

The **delete cos mac_mapping** command is used to delete the CoS MAC mapping method on the Switch.

delete cos mac_mapping	
Syntax	**delete cos mac_mapping destination_addr <macaddr>**
Parameter	*<macaddr>* - Specifies the mapped MAC address to be deleted.

config cos ip_mapping

The **config cos ip_mapping** command is used to configure the CoS IP mapping method on the Switch.

config cos ip_mapping	
Syntax	**config cos ip_mapping destination_ip <ipaddr> class <class_id 0-3>**
Parameter	*<ipaddr>* - Specifies the IP address to be mapped. For example, 10.90.90.99. *<class_id 0-3>* - Specifies the number of the Switch's hardware priority queue.

show cos ip_mapping

The **show cos ip_mapping** command is used to displays the CoS IP mapping information on the Switch.

show cos ip_mapping	
Syntax	**show cos ip_mapping {destination_ip <ipaddr>}**
Parameter	<*ipaddr*> - Displays the information regarding to the CoS IP mapping.

delete cos ip_mapping

The **delete cos ip_mapping** command is used to delete the CoS IP mapping on the Switch.

delete cos ip_mapping	
Syntax	**delete cos ip_mapping destination_ip <ipaddr>**
Parameter	<*ipaddr*> - Specifies the mapped IP address to be deleted.

config cos tcp_port_mapping

The **config cos tcp_port_mapping** command is used to configure the CoS TCP port mapping on the Switch.

config cos tcp_port_mapping	
Syntax	**config cos tcp_port_mapping destination_port <value 0-65535> class <class_id 0-3>**
Parameter	<*value 0-65535*> - Specifies the tcp port number to be mapped. <*class_id 0-3*> - Specifies the number of the Switch's hardware priority queue.

show cos tcp_port_mapping

The **show cos tcp_port_mapping** command displays the CoS TCP port mapping information on the Switch.

show cos tcp_port_mapping	
Syntax	**show cos tcp_port_mapping {destination_port <value 0-65535>}**
Parameter	<*value 0-65535*> - Specifies the mapped tcp port information to be displayed.

delete cos tcp_port_mapping

The **delete cos tcp_port_mapping** command is used to delete the CoS TCP port mapping method on the Switch.

delete cos tcp_port_mapping	
Syntax	**delete cos tcp_port_mapping destination_port <value 0-65535>**
Parameter	<*value 0-65535*> - Specifies the CoS TCP port mapped to be deleted.

config cos udp_port_mapping

The **config cos udp_port_mapping** command is used to configure the CoS UDP mapping method on the Switch.

config cos udp_port_mapping	
Syntax	**config cos udp_port_mapping destination_port <value 0-65535> class <class_id 0-3>**
Parameter	<*value 0-65535*> - Specifies the udp port number to be mapped.

<*class_id 0-3*> - Specifies the number of the Switch's hardware priority queue.

show cos udp_port_mapping

The **show cos udp_port_mapping** command is used to display the CoS UDP port mapping information between an incoming packet's 802.1p priority value on the Switch.

show cos udp_port_mapping	
Syntax	**show cos udp_port_mapping {destination_port <value 0-65535>}**
Parameter	<*value 0-65535*> - Specifies the udp port information to be displayed.

delete cos udp_port_mapping

The **delete cos udp_port_mapping** command is used to delete the CoS UDP port mapping between an incoming packet's 802.1p priority value.

delete cos udp_port_mapping	
Syntax	**delete cos udp_port_mapping destination_port <value 0-65535>**
Parameter	<*value 0-65535*> - Specifies the mapped udp port to be deleted.

config cos vlanid_mapping

The **config cos vlanid_mapping** command is used to configure the CoS VLAN id mapping method on the Switch.

config cos vlanid_mapping	
Syntax	**config cos vlanid_mapping vid <vlanid 1-4094> class <class_id 0-3>**
Parameter	<*vlanid 1-4094*> - Specifies the vlan id to be mapped. <*class_id 0-3*> - Specifies the number of the Switch's hardware priority queue.

show cos vlanid_mapping

The **show cos vlanid_mapping** command is used to display the CoS VLAN id mapping information between an incoming packet's 802.1p priority value.

show cos vlanid_mapping	
Syntax	**show cos vlanid_mapping {vid <vlanid 1-4094>}**
Parameter	<*vlanid 1-4094*> - Specifies the mapped vlan id information to be displayed.

delete cos vlanid_mapping

The **delete cos vlanid_mapping** command is used to delete the mapping between an incoming packet's 802.1p priority value.

delete cos vlanid_mapping	
Syntax	**delete cos vlanid_mapping vid <vlanid 1-4094>**
Parameter	<*vlanid 1-4094*> - Specifies the mapped vlan id to be deleted.

config cos protocol_mapping

The **config cos protocol_mapping** command is used to configure the CoS protocol mapping method on the Switch.

config cos protocol_mapping

Syntax	**config cos protocol_mapping protocol <ip_protocol 1-255> class <class_id 0-3>**
Parameter	*<ip_protocol 1-255>* - Specifies the protocol IP to be mapped. *<class_id 0-3>* - Specifies the number of the Switch's hardware priority queue.

show cos protocol_mapping

The **show cos protocol_mapping** command is used to display the CoS protocol mapping information between an incoming packet's 802.1p priority value.

show cos protocol_mapping

Syntax	**show cos protocol_mapping {protocol <ip_protocol 1-255>}**
Parameter	*<ip_protocol 1-255>* - Specifies the mapped protocol IP to be displayed.

delete cos protocol_mapping

The **delete cos protocol_mapping** command is used to delete the CoS protocol mapping between an incoming packet's 802.1p priority value.

delete cos protocol_mapping

Syntax	**delete cos protocol_mapping protocol <ip_protocol 1-255>**
Parameter	*<ip_protocol 1-255>* - Specifies the mapped protocol IP to be deleted.

config 802.1p user_priority

The **config 802.1p user_priority** command configures the way the Switch maps an incoming packet, based on its 802.1p user priority tag, to one of the four hardware priority classes of service available on the Switch.

config 802.1p user_priority

Syntax	**config 802.1p user_priority <priority 0-7> <class_id 0-3>**
Parameter	*<priority 0-7>* − The 802.1p priority value (0 to 7) to map to one of the Switch's four hardware priority classes of service. *<class_id 0-3>* − The Switch's hardware priority class of service (0 to 3) to map to the 802.1p priority value specified above. The Switch's default is to map the incoming 802.1p priority values to the four hardware classes of service according to the following chart:

802.1p value	Switch Priority Queue	Switch Priority Queue(stack)
0	1	0
1	0	0
2	0	0
3	1	0
4	2	1
5	2	1
6	3	2
7	3	2

show 802.1p user_priority

The **show 802.1p user_priority** command displays the current mapping of an incoming packet's 802.1p priority value to one of the Switch's four hardware priority queues.

show 802.1p user_priority

Syntax	**show 802.1p user_priority**
Parameter	None.

config 802.1p default_priority

The **config 802.1p default_priority** command specifies the 802.1p priority value an untagged, incoming packet is assigned before being forwarded to its destination.

config 802.1p default_priority	
Syntax	**config 802.1p default_priority [<portlist> | all] <priority 0-7>**
Parameter	*<portlist>* − A port or range of ports to be configured. *all* − Specifies that the config 802.1p default_priority command applies to all ports on the Switch. *<priority 0-7>* − The 802.1p priority value that an untagged, incoming packet is granted before being forwarded to its destination.

show 802.1p default_priority

The **show 802.1p default_priority** command displays the currently configured 802.1p priority value that is assigned to an incoming, untagged packet before being forwarded to its destination.

show 802.1p default_priority	
Syntax	**show 802.1p default_priority**
Parameter	None.

config scheduling mechanism

The **config scheduling_mechanism** command configures the scheduling mechanism for the QoS function. It allows the user to select between a round robin (WRR) and a strict mechanism for emptying the priority classes of service of the QoS function. The Switch contains four hardware priority classes of service. Incoming packets must be mapped to one of these four hardware priority classes of service, or queues. This command is used to specify the rotation by which these four hardware priority queues are emptied.

The Switch's default is to empty the four hardware priority queues in order − from the highest priority hardware queue (class 3) to the lowest priority hardware queue (class 0). Each queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. A lower priority hardware queue will be pre-empted from emptying its queue if a packet is received on a higher priority hardware queue. The packet received on the higher priority hardware queue transmits its packet before allowing the lower priority hardware queue to resume clearing its queue.

config scheduling_mechanism	
Syntax	**config scheduling_mechanism [strict | wrr]**
Parameter	*strict* – Specifies that the highest class of service is the first to be processed. That is, the highest class of service should finish emptying before the others begin. *wrr* – Specifies that the priority classes of service are to empty packets in a weighted roundrobin (WRR) order.

show scheduling mechanism

The **show scheduling_mechanism** command displays the current traffic scheduling mechanisms in use on the Switch.

show scheduling_mechanism	
Syntax	**show scheduling_mechanism**
Parameter	None.

config dscp_mapping

The **config dscp_mapping** command enables mapping the DSCP value (the priority) to a specific queue (the class_id).

config dscp_mapping	
Syntax	**config dscp_mapping dscp_value <value 0-63> class <class_id 0-3>]**
Parameter	<*value 0-63*> –The selected value of priority. The value may be between 0 and 63. <*class_id 0-3*> – The class_id (queue) mapped to the priority. The value may be between 0 and 3.

show dscp_mapping

The **show dscp_mapping** command displays the class_ids assigned to each user priority.

show dscp_mapping	
Syntax	**show dscp_mapping {dscp_value <value 0-63>}**
Parameter	<*value 0-63*> –The selected value of priority will be dispalyed. The value may be between 0 and 63.

16 *RMON Commands*

The RMON commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable rmon	
disable rmon	
create rmon alarm	<alarm_index 1-65535> <OID_variable 255> rm_index <interval 1-2147482647> [absolute | delta] rising-threshold <value 0-2147483647> <rising_event_index 1-65535> falling-threshold <value 0-2147483647> <falling_event_index 1-65535> [owner <owner_string 127>]
create rmon collection stats	<stats_index 1-65535> port <ifindex> owner <owner_string 127>
create rmon collection history	<hist_index 1-65535> port <ifindex> buckets <buckets_req 1-50> interval <interval 1-3600> owner <owner_string 127>
create rmon event	<event_index 1-65535> description <desc_string 127> {[log | owner <owner_string 127> | trap <community_string 127>]}

Each command is listed in detail, as follows:

enable rmon

The **enable rmon** command enables remote monitoring (RMON) statusfor the SNMP function on the Switch.

enable rmon	
Syntax	**enable rmon**
Parameter	None.

disable rmon

The **disable rmon** command disables remote monitoring (RMON) statusfor the SNMP function on the Switch.

disable rmon	
Syntax	**disable rmon**
Parameter	None.

create rmon alarm

The **create rmon alarm** command allows the user to configure the network alarms. Network alarms occur when a network problem, or event, is detected.

create rmon alarm	
Syntax	**create rmon alarm <alarm_index 1-65535> <OID_variable 255> rm_index <interval 1-2147482647> [absolute | delta] rising-threshold <value 0-2147483647> <rising_event_index 1-65535> falling-threshold <value 0-2147483647> <falling_event_index 1-65535> [owner <owner_string 127>]**
Parameter	<alarm_index> − Specifies the alarm number. *<OID_variable 255>* − Specifies the MIB variable value. *rm_index <interval 1-2147482647>* − Specifies the alarm interval time in seconds. *[absolute | delta]* − Specifies the sampling method for the selected

variable and comparing the value against the thresholds. The possible values are absolute and delta:

- *absolute* –Compares the values directly with the thresholds at the end of the sampling interval.
- *delta* –Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.

rising-threshold <*value 0-2147483647*> − Specifies the rising counter value that triggers the rising threshold alarm.

<*rising_event_index 1-65535*> − Specifies the event that triggers the specific alarm.

falling-threshold <*value 0-2147483647*> − Specifies the falling counter value that triggers the falling threshold alarm.

<*falling_event_index 1-65535*> − Specifies the event that triggers the specific alarm. The possible field values are user defined RMON events.

owner <*owner_string 127*> − Specifies the device or user that defined the alarm.

create rmon collection stats

The **create rmon collection stats** command allows user to configure the rmon stats settings on the Switch.

create rmon collection stats	
Syntax	**create rmon collection stats <stats_index 1-65535> port <ifindex> owner <owner_string 127>**
Parameter	<*stats_index 1-65535*> − Specifies the stats number. *port* <*ifindex*> − Specifies the port from which the RMON information was taken. *owner* <*owner_string 127*> − Specifies the device or user that defined the stats.

create rmon collection history

The **create rmon collection history** command allows user to configure the rmon history settings on the Switch.

create rmon collection history	
Syntax	**create rmon collection history <hist_index 1-65535> port <ifindex> buckets <buckets_req 1-50> interval <interval 1-3600> owner <owner_string 127>**
Parameter	<*hist_index 1-65535*> − Indicates the history control entry number. *port* <*ifindex*> − Specifies the port from which the RMON information was taken. *buckets* <*buckets_req 1-50*> − Specifies the number of buckets that the device saves. *interval* <*interval 1-3600*> − Specifies in seconds the time period that samplings are taken from the ports. The field range is *1-3600*. The default is *1800* seconds (equal to 30 minutes). *owner* <*owner_string 127*> − Specifies the RMON station or user that requested the RMON information.

create rmon event

The **create rmon event** command provides user to configure the settings of rmon event on the Switch.

create rmon event	
Syntax	**create rmon event <event_index 1-65535> description <desc_string 127> {[log | owner <owner_string 127> | trap <community_string 127>]}**
Parameter	*<event_index 1-65535>* − Specifies the event number. *description <desc_string 127>* − Specifies the user-defined event description. *log* − Indicates that the event is a log entry. *owner <owner_string 127>* − Specifies the time that the event occurred. *trap <community_string 127>* − Specifies the community to which the event belongs.

17 *TRUSTED HOST Commands*

The Trusted Host commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable trusted_host	
disable trusted_host	
create trusted_host	<ipaddr>
show trusted_host	
delete trusted_host	<ipaddr>

Each command is listed in detail, as follows:

enable trusted_host

The **enable trusted_host** command enables trusted host support on the Switch.

enable trusted_host	
Syntax	**enable trusted_host**
Parameter	None.

disable trusted_host

The **disable trusted_host** command disables trusted host support on the Switch.

disable trusted_host	
Syntax	**disable trusted_host**
Parameter	None.

create trusted host

The **create trusted_host** command creates a trusted host. The Switch allows specifying up to 30 IP addresses that are allowed to manage the Switch via in-band based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the Switch, provided the user knows the Username and Password.

create trusted_host	
Syntax	**create trusted_host <ipaddr>**
Parameter	*<ipaddr>* − The IP address of the trusted host to be created. For example, 10.90.90.99.

show trusted host

The **show trusted_host** command displays a list of trusted hosts entered on the Switch using the **create trusted_host** command above.

show trusted_host	
Syntax	**show trusted_host**
Parameter	None.

delete trusted host

The **delete trusted_host** command deletes a trusted host entry made using the **create trusted_host** command above.

delete trusted_host	
Syntax	**delete trusted_host <ipaddr>**
Parameter	*<ipaddr>* − The IP address of the trusted host.

18 *PORT MIRRORING Commands*

The Port Mirroring commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config mirror	target <port 1-*maxport*> source <port 1-*maxport* > direction [ingress | egress | both]
delete mirror	target <port 1-*maxport* > source <port 1-*maxport* >
show mirror	

Each command is listed in detail, as follows:

config mirror

The **config mirror** command allows a port to have all of its traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, one can specify that only traffic received by or sent by one or both is mirrored to the target port.

config mirror	
Syntax	**config mirror target <port 1- *maxport* > source <port 1- *maxport* > direction [ingress | egress | both]**
Parameter	*target <port 1-maxport>* − Specifies the port that mirrors traffic forwarding. *source <port 1-maxport>* – Specifies the port or ports being mirrored. This cannot include the target port. *ingress* – Allows mirroring of packets received by (flowing into) the source port. *egress* – Allows mirroring of packets sent to (flowing out of) the source port. *both* – Allows mirroring of all the packets received or sent by the source port. *Comment*: The user can define up to 8 source ports and one destination port. One source port can be configured each time using one CLI command, So in order to configure multiple source ports, multiple CLI commands should be used.

Note: The syntax maxport for DES-1210-10 is 10 and 28 for DES-1210-28.

delete mirror

The **delete mirror** command removes a previously configured mirror port − source port pair on the Switch.

delete mirror	
Syntax	**delete mirror target <port 1- *maxport* > source <port 1- *maxport*>**
Parameter	*target <port 1- maxport>* − Specifies the port that mirrors traffic forwarding. *source <port 1- maxport>* – Specifies the port or ports being mirrored. This cannot include the target port.

show mirror

The **show mirror** command displays the current port mirroring configuration on the Switch.

show mirror	
Syntax	**show mirror**
Parameter	None.

19 VLAN Commands

The VLAN commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create vlan	<string 20> {tag <integer 2-4094> | type_1q_vlan_advertisement}
delete vlan	[<vlan_name 32> | vlanid <integer 2-4094>]
config vlan	<vlan_name 32> [add [tagged | untagged | forbidden] | delete <portlist> | advertisement [disable | enable]]
config vlan vlanid	<integer 1-4094> [add [tagged | untagged | forbidden] | delete <portlist> | advertisement [disable | enable]]
config gvrp	[<portlist> | timer | all] { state [enable | disable] { ingress_checking [enable | disable] | acceptable_frame [Tagged_Only | All_Frames] | pvid <vlanid 1-4094>}
enable gvrp	
disable gvrp	
show vlan	{<integer 1-4094>}
show gvrp	{<portlist> | timer}
enable asymmetric_vlan	
disable asymmetric_vlan	
show asymmetric_vlan	
enable management vlan	
disable management vlan	
config management vlan	<string 32>
show management vlan	
config voicevlan	[default_OUI [3COM | Avaya | Cisco | Huawei3COM | NEC/Pilips | Pingtel | Siemens | Veritel] | UserDefine_OUI <string 20> <mac_addr> | auto_detection ports <portlist>[disable | enable]]
show voicevlan	[oui | ports setting]

Each command is listed in detail, as follows:

create vlan

The **create vlan** command creates a VLAN on the Switch.

create vlan	
Syntax	**create vlan <string 20> {tag <integer 2-4094> | type_1q_vlan_advertisement}**
Parameter	*<string 20>* − The name of the VLAN to be created. *tag <integer 2-4094>* − The VLAN ID of the VLAN to be created. The allowed values range from 2 to 4094. *type_1q_vlan_advertisement* − Specifies the 1q vlan advertisement on the Switch.

delete vlan

The **delete vlan** command deletes a previously configured VLAN on the Switch.

delete vlan	
Syntax	**delete vlan [<vlan_name 32> | vlanid <integer 2-4094>]**
Parameter	*<vlan_name 32>* − The name of the VLAN to be deleted. *vlanid <integer 2-4094>* − The VLAN ID of the VLAN to be deleted. The allowed values range from 2 to 4094.

config vlan

The **config vlan** command allows the user to add or delete ports to the port list of a previously configured VLAN. You can specify the additional ports as tagging, untagging, or forbidden. The default is to assign the ports as untagged.

config vlan	
Syntax	**config vlan <vlan_name 32> [add [tagged | untagged | forbidden] | delete <portlist> | advertisement [disable | enable]]**
Parameter	*<vlan_name 32>* − The name of the VLAN to be configured. *add* − Specifies that ports are to be added to a previously created vlan. *delete* − Specifies that ports are to be deleted from a previously created vlan. *tagged* − Specifies the additional ports as tagged. *untagged* − Specifies the additional ports as untagged. *forbidden* − Specifies the additional ports as forbidden. *<portlist>* − A port or range of ports to be added to or deleted from the VLAN. *advertisement* − Specifies that the vlan advertisement is enabled or disabled.

config vlan vlanid

The **config vlan vlanid** command allows the user to add or delete ports to the port list of a previously configured VLAN. You can specify the additional vlan id as tagging, untagging, or forbidden. The default is to assign the ports as untagged.

config vlan vlanid	
Syntax	**config vlan vlanid <integer 1-4094> [add [tagged | untagged | forbidden] | delete <portlist> | advertisement [disable | enable]]**
Parameter	*vlanid <integer 1-4094>* − Specifies the VLAN id to be configured. *add* − Specifies that ports are to be added to a previously created vlan. *delete* − Specifies that ports are to be deleted from a previously created vlan. *tagged* − Specifies the additional ports as tagged. *untagged* − Specifies the additional ports as untagged. *forbidden* − Specifies the additional ports as forbidden. *<portlist>* − A port or range of ports to be added to or deleted from the VLAN. *advertisement* − Specifies that the vlan advertisement is enabled or disabled.

config gvrp

The **config gvrp** command configures the Group VLAN Registration Protocol on the Switch. The user can configure ingress checking and acceptable frame tagged only, the sending and receiving of GVRP information, and the Port VLAN ID (PVID).

config gvrp

Syntax	**config gvrp [<portlist> | timer | all] { state [enable | disable] { ingress_checking [enable | disable] | acceptable_frame [Tagged_Only | All_Frames] | pvid <vlanid 1-4094>}**
Parameter	*<portlist>* − A port or range of ports for which to configure GVRP. *timer* − configure timer on ports. *all* − configure GVRP on ports. *state [enable* | *disable]* - enable and disable GVRP. *ingress_checking [enable* | *disable]* − Enables or disables ingress checking for the specified port list. *acceptable_frame [Tagged_only* | *All_Frames]* – Defines the type of frame accepted. Acceptable frames can be limited to tagged frames only (*tagged_only*) or can accept tagged and untagged (*admit_all*). *pvid <vlanid 1-4094>* – Specifies the default VLAN associated with the port, by VLAN ID.

enable gvrp

The **enable gvrp** command, along with the **disable gvrp** command below, is used to enable and disable GVRP on the Switch, without changing the GVRP configuration on the ports and the LAGs.

enable gvrp	
Syntax	**enable gvrp**
Parameter	None.

disable gvrp

The **disable gvrp** command, along with the **enable gvrp** command above, is used to enable and disable GVRP on the Switch, without changing the GVRP configuration on the ports and the LAGs.

disable gvrp	
Syntax	**disable gvrp**
Parameter	None.

show vlan

The **show vlan** command displays summary information about each VLAN including the VLAN ID, VLAN name, the Tagging/Untagging status, and the Member/Non-member/Forbidden status of each port that is a member of the VLAN.

show vlan	
Syntax	**show vlan {<integer 1-4094>}**
Parameter	*<integer 1-4094>* − The id of the VLAN whose settings are to be displayed.

show gvrp

The **show gvrp** command displays the GVRP status for a port list or a port channel on the Switch.

show gvrp	
Syntax	**show gvrp {<portlist> | timer}**
Parameter	*<portlist>* − A port or range of ports for which to configure GVRP. *timer* − Displays timer on ports.

enable asymmetric vlan

The **enable asymmetric_vlan** command is used to enable Asymmetric VLAN on the Switch.

enable asymmetric_vlan	
Syntax	**enable asymmetric_vlan**
Parameter	None.

disable asymmetric vlan

The **disable asymmetric_vlan** command is used to disable Asymmetric VLAN on the Switch.

disable asymmetric_vlan	
Syntax	**disable asymmetric_vlan**
Parameter	None.

show asymmetric vlan

The **show asymmetric_vlan** command is used to display Asymmetric VLAN on the Switch.

show asymmetric_vlan	
Syntax	**show asymmetric_vlan**
Parameter	None.

enable management vlan

The **enable management vlan** command enables the management VLAN on the Switch.

enable management vlan	
Syntax	**enable management vlan**
Parameter	None.

disable management vlan

The **disable management vlan** command disables the management VLAN on the Switch.

disable management vlan	
Syntax	**disable management vlan**
Parameter	None.

config management vlan

The **config management vlan** command configures the management VLAN on the Switch.

config management vlan	
Syntax	**config management vlan <string 32>**
Parameter	*<string 32>* − Specifies the management VLAN name on the Switch.

show management vlan

The **show management vlan** command displays the management VLAN information on the Switch.

show management vlan	
Syntax	**show management vlan**
Parameter	None.

config voicevlan

The **config voice vlan** command configures the various parameters of Voice VLAN.

config voicevlan

Syntax	**config voicevlan [default_OUI [3COM | Avaya | Cisco | Huawei3COM | NEC/Pilips | Pingtel | Siemens | Veritel] | UserDefine_OUI <string 20> <mac_addr> | auto_detection ports <portlist>[disable | enable]]**
Parameter	*default_OUI* − Pre-defined OUI values, including brand names of 3COM, Avaya, Cisco, Huawei3COM, NEC/Pilips, Pingtel, Siemens, and Veritel. *UserDefine_OUI* <*string 20*> − Specifies the OUI name of the switch. <*mac_addr*> − adds the specified MAC address to the voice VLAN OUI table. (Length: 3 bytes) <*portlist*> − A port or range of ports for which to configure for the voice vlan table.

show voicevlan

The **show voice vlan** command displays the Voice VLAN status on the Switch.

config voicevlan	
Syntax	**show voicevlan [oui | ports setting]**
Parameter	*oui* − Displays voice vlan OUI table. *ports setting* − Displays voice vlan port setting status of the switch.

20 LINK AGGREGATION Commands

The Link Aggregation commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create link_aggregation	group_id <value 1-*maxgroup* > {type [lacp | static]}
delete link_aggregation	group_id <value 1-*maxgroup* >
config link_aggregation	group_id <value 1-*maxgroup* > { [master_port <port 1-*maxport*> | ports <portlist>] | state [enable | disable] | algorithm [ip_source | ip_destination | ip_source_dest | mac_destination | mac_source | mac_source_dest] }
show link_aggregation	{group_id <value 1-*maxgroup*>}{algorithm}

Note: The syntax maxgroup for DES-1210-10 is 5 and 8 for DES-1210-28.

DES-1210-10 allows up to 5 link aggregation groups to be configured and DES-1210-28 allows up to 8 link aggregation groups to be configured.

Each command is listed in detail, as follows:

create link_aggregation

The **create link_aggregation** command creates a link aggregation group with a unique identifier.

create link_aggregation	
Syntax	**create link_aggregation group_id <value 1-*maxgroup*> {type [lacp | static]}**
Parameter	*group_id <value 1-8>* − Specifies the group ID. The Switch allows up to 5 link aggregation groups to be configured. The group number identifies each of the groups. *type* – Specify the type of link aggregation used for the group. If the type is not specified the default type is *static*. • *lacp* – This designates the port group as LACP compliant. LACP allows dynamic adjustment to the aggregated port group. LACP compliant ports may be further configured (see config lacp_ports). LACP compliant must be connected to LACP compliant devices. The maximum ports that can be configure in the same LACP are 16. • *static* – This designates the aggregated port group as static. Static port groups can not be changed as easily as LACP compliant port groups since both linked devices must be manually configured if the configuration of the trunked group is changed. If static link aggregation is used, be sure that both ends of the connection are properly configured and that all ports have the same speed/duplex settings. The maximum ports that can be configure in the same static LAG are 8.

delete link_aggregation

The **delete link_aggregation** command deletes a link aggregation group with a unique identifier.

delete link_aggregation	
Syntax	**delete link_aggregation group_id <value 1-*maxgroup* >**

Parameter	*group_id <value 1-8>* − Specifies the group ID. The Switch allows up to 8 link aggregation groups to be configured. The group number identifies each of the groups.

config link_aggregation

The **config link_aggregation** command configures a link aggregation group created with the **create link_aggregation** command above.

config link_aggregation	
Syntax	**config link_aggregation group_id <value 1-*maxgroup*> { [master_port <port 1-*maxport*> | ports <portlist>] | state [enable | disable] | algorithm [ip_source | ip_destination | ip_source_dest | mac_destination | mac_source | mac_source_dest] }**
Parameter	*group_id <value 1-8>* − Specifies the group ID. The Switch allows up to 8 link aggregation groups to be configured. The group number identifies each of the groups. *<port 1-maxport>* − Specifies the port to be configured. *ports <portlist>* − Specifies a list of ports to belong to the link aggregation group. Ports will be listed in only one aggregation group and link aggregation groups can not overlap to each other. The user must cofigure at list two ports in LAG. *state [enable | disable]* − Enables or disables the specified link aggregation group. *algorithm* – Specifies the source or destination for the link aggregation hash algorithm, MAC address or IP address.

Note: The syntax maxport for DES-1210-10 is 10 and 28 for DES-1210-28.

show link_aggregation

The **show link_aggregation** command displays the current link aggregation configuration of the Switch.

show link_aggregation	
Syntax	**show link_aggregation {group_id <value 1-*maxgroup*>}{algorithm}**
Parameter	*group_id <value 1-8>* − Specifies the group ID. The Switch allows up to 8 link aggregation groups to be configured. The group number identifies each of the groups. *algorithm* – shows which hash Algorithm is used for link aggregation distribution.

21 BASIC IP Commands

The Basic IP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config ipif system	[{ipaddress <network_address> gateway <ip_addr> | state [enable | disable]} | dhcp | dhcp_option12 [clear_hostname | hostname <hostname 63>]]
show ipif	

Each command is listed in detail, as follows:

config ipif system

The **config ipif system** command configures the System IP interface on the Switch.

config ipif system	
Syntax	**config ipif system [{ipaddress <network_address> gateway <ip_addr> | state [enable | disable]} | dhcp | dhcp_option12 [clear_hostname | hostname <hostname 63>]]**
Parameter	*system* - The IP interface name to be configured. The default IP Interface name on the Switch is 'System'. All IP interface configurations done are executed through this interface name. *<network_address>* − IP address and netmask of the IP interface to be created. The address and mask information may be specified by using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16). *<ip_addr>* - Specifies the gateway IP address for the switch. *state [enable* | *disable]* − Enables or disables the IP interface. *dhcp* − Specified the Switch to use DHCP. *clear_hostname* − Clears the host name of DHCP. *hostname <hostname 63>* − Specifies the host name of DHCP.

show ipif

The **show ipif** command displays the configuration of an IP interface on the Switch.

show ipif	
Syntax	**show ipif**
Parameter	None.

22 IGMP SNOOPING Commands

The IGMP Snooping commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config igmp_snooping	[<vlan_name 32> | multicast_vlan | multicast_vlan_group] {fast_leave [enable | disable] | host_timeout <sec 130-153025> | router_timeout <sec 60-600> | leave_timer <sec 1-25> | state [enable | disable]}
config igmp_snooping querier	vlan <vlan_name 32> state [enable | disable] {querier_version [IGMPv2 | IGMPv3]}
config router_ports	<vlan_name 32> [add | delete] <portlist>
config router_ports_forbidden	<vlan_name 32> [add | delete] <portlist>
enable igmp_snooping	{multicast_vlan}
disable igmp_snooping	{multicast_vlan}
show igmp_snooping	{vlan | multicast_vlan | multicast_vlan_group [<vlan_name 32>]}
show igmp_snooping group	{vlan <vlan_name 32>}
show igmp_snooping forwarding	{vlan <vlan_name 32>}
config igmp access_authentication	ports [all | <portlist>] state [enable | disable]
show igmp access_authentication	ports [all | <portlist>]
show router_port	{vlan <vlan_name 32> | static | dynamic | forbidden}

Each command is listed in detail, as follows:

config igmp_snooping

The **config igmp_snooping** command configures IGMP snooping on the Switch.

config igmp_snooping	
Syntax	**config igmp_snooping [<vlan_name 32> | multicast_vlan | multicast_vlan_group] {fast_leave [enable | disable] | host_timeout <sec 130-153025> | router_timeout <sec 60-600> | leave_timer <sec 1-25> | state [enable | disable]}**
Parameter	*<vlan_name 32>* − The name of the VLAN for which IGMP snooping is to be configured. *multicast_vlan* – Specifies that IGMP snooping is to be configured for multicast VLANs on the Switch. *multicast_vlan_group* – Specifies that IGMP snooping is to be configured for multicast vlan groups on the Switch. *fast_leave [enable | disable]* − Specifies the fast leave status is enabled or disabled on the switch. *host_timeout <sec 130-153025>* − Specifies the maximum amount of time a host can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds. *router_timeout <sec 60-600>* − Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds.

leave_timer <*sec 1-25*> − Leave timer. The default is 10 seconds.

state [enable | *disable]* − Enables or disables IGMP snooping for the specified VLAN.

config igmp_snooping querier

The **config igmp_snooping querier** command configures IGMP snooping querier on a specific VLAN.

config igmp_snooping querier	
Syntax	**config igmp_snooping querier vlan <vlan_name 32> state [enable | disable] {querier_version [IGMPv2 | IGMPv3]}**
Parameter	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping is to be configured. Up to 32 characters can be used. *state [enable*	*disable]* − Enables/Disables IGMP Snooping Querier. *querier_version [IGMPv2*	*IGMPv3]* − Specifies the IGMP Querier version on the VLAN.

config router_ports

The **config router_ports** command designates a range of ports as being connected to multicast-enabled routers. This ensures all packets with such a router as its destination will reach the multicast-enabled router − regardless of protocol, etc.

config router_ports	
Syntax	**config router_ports <vlan_name 32> [add | delete] <portlist>**
Parameter	<*vlan_name 32*> − The name of the VLAN on which the router port resides. Up to 32 characters can be used. *[add*	*delete]* – Specifies whether to add or delete ports defined in the following parameter <portlist>, to the router port function. <*portlist*> − A port or range of ports that will be configured as router ports.

config router_ports_forbidden

The **config router_ports_forbidden** command denies a range of ports access to multicast–enabled routers. This ensures all packets with such a router as its destination will not reach the multicast–enabled router − regardless of protocol, etc.

config router_ports_forbidden	
Syntax	**config router_ports_forbidden <vlan_name 32> [add | delete] <portlist>**
Parameter	<*vlan_name 32*> − The name of the VLAN on which the router port resides. Up to 32 characters can be used. *[add*	*delete]* – Specifies whether to add or delete ports defined in the following parameter <portlist>, to the router port forbidden function. <*portlist*> − A port or range of ports that will be configured as router ports.

enable igmp_snooping

The **enable igmp_snooping** command enables IGMP snooping on the Switch.

enable igmp_snooping	
Syntax	**enable igmp_snooping {multicast_vlan}**
Parameter	*{multicast_vlan}* − Enables the multicast VLAN for IGMP Snooping on the Switch.

disable igmp_snooping

The **disable igmp_snooping** command disables IGMP snooping on the Switch.

disable igmp_snooping	
Syntax	**disable igmp_snooping {multicast_vlan}**
Parameter	*{multicast_vlan}* − Disables the multicast VLAN for IGMP Snooping on the Switch.

show igmp_snooping

The **show igmp_snooping** command displays the current IGMP snooping configuration on the Switch.

show igmp_snooping	
Syntax	**show igmp_snooping {vlan | multicast_vlan | multicast_vlan_group [<vlan_name 32>]}**
Parameter	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping configuration is to be displayed. Up to 32 characters can be used.

show igmp_snooping group

The **show igmp_snooping group** command displays the current IGMP snooping group configuration on the Switch.

show igmp_snooping group	
Syntax	**show igmp_snooping group {vlan <vlan_name 32>}**
Parameter	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping configuration is to be displayed. Up to 32 characters can be used.

show igmp_snooping forwarding

The **show igmp_snooping forwarding** command displays the current IGMP snooping forwarding information on the Switch.

show igmp_snooping forwarding	
Syntax	**show igmp_snooping forwarding {vlan <vlan_name 32>}**
Parameter	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping configuration is to be displayed. Up to 32 characters can be used.

config igmp access_authentication

The **config igmp access_authentication** command configures the IGMP access authentication on the Switch.

config igmp access_authentication	
Syntax	**config igmp access_authentication ports [all | <portlist>] state [enable | disable]**
Parameter	*all* − Specifies all ports to be configured. *<portlist>* − A port or range of ports to be configured on the Switch. *state [enable | disable]* − Specifies the state for the port to be disabled or enabled.

show igmp access_authentication

The **show igmp access_authentication** command displays the IGMP access authentication configuration on the Switch.

show igmp access_authentication

Syntax	**show igmp access_authentication ports [all | <portlist>]**
Parameter	*all* − Specifies all ports to be displayed. *<portlist>* − A port or range of ports to be displayed on the Switch.

show router_ports

The **show router_port** command displays the router ports currently configured on the Switch.

show router_port	
Syntax	**show router_port {vlan <vlan_name 32> | static | dynamic | forbidden}**
Parameter	*vlan <vlan_name 32>* − The name of the VLAN on which the router port resides. Up to 32 characters can be used. *static* − Displays router ports that have been statically configured. *dynamic* − Displays router ports that have been dynamically learned. *forbidden* − Displays router ports that have been forbidden configured.

23 *802.1X Commands*

The 802.1x commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable 802.1x	
disable 802.1x	
show 802.1x auth_state	{ports <portlist>}
show 802.1x auth_configuration	{ports <portlist>}
config 802.1x auth_parameter ports	[<portlist> | all] [default | { port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 300-4294967295> | direction [both | in] | enable_reauth [enable | disable]}]
config 802.1x init	port_based ports [<portlist> | all]
config 802.1x auth_protocol	[radius_eap | local]
config 802.1x reauth	port_based ports [<portlist> | all]
config radius add	[<server_index 1-3>][<server_ip>] [key <passwd 32>] [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | retransmit <int 1-255>}]
config radius delete	[<server_index 1-3>]
config radius	<server_index 1-3> {key <passwd 32> | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | ipaddress <server_ip> | retransmit <int 1-255> | timeout <int 1-255>}
show radius	
config 802.1x auth_mode	[port_based | mac_based]
create 802.1x user	<username 15>
delete 802.1x user	<username 15>
show 802.1x user	<username 15>
create 802.1x guest vlan	<vlan_name 32>
delete 802.1x guest vlan	<vlan_name 32>
config 802.1x guest_vlan ports	<portlist> state [enable | disable]
show 802.1x guest_vlan	

Each command is listed in detail, as follows:

enable 802.1x

The **enable 802.1x** command enables the 802.1x Port-based Network Access control server application on the Switch.

enable 802.1x	
Syntax	**enable 802.1x**
Parameter	None.

disable 802.1x

The **disable 802.1x** command disables the 802.1x Port-based Network Access control server application on the Switch.

disable 802.1x	
Syntax	**disable 802.1x**
Parameter	None.

show 802.1x auth_state

The **show 802.1x auth_state** command displays the current 802.1x authentication state of the specified ports of the Port-based Network Access Control server application on the Switch.

The following details are displayed:

Port number: Shows the physical port number on the Switch.

Auth PAE State: Initialize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth − Shows the current state of the Authenticator PAE.

Backend State: Request / Response / Fail / Idle / Initialize / Success / Timeout − Shows the current state of the Backend Authenticator.

Port Status: Authorized / Unauthorized − Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.

show 802.1x auth_state	
Syntax	**show 802.1x auth_state {ports <portlist>}**
Parameter	*ports <portlist>* − A port or range of ports whose settings are to be displayed.

show 802.1x auth_configuration

The **show 802.1x auth_configuration** command displays the current configuration of the 802.1x server on the Switch.

The following details are displayed:

802.1x: Enabled/Disabled − Shows the current status of 802.1x functions on the Switch.

Authentication Mode: Port-based/Mac-based/None − Shows the 802.1x authorization mode.

Capability: Remote/none − Shows the type of capability in use between the Switch and a RADIUS server.

Port number: Shows the physical port number on the Switch.

AdminCrlDir: Both/In − Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.

OpenCrlDir: Both/In − Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.

Port Control: ForceAuth/ForceUnauth/Auto − Shows the administrative control over the port's authorization status. ForceAuth forces the Authenticator of the port to become Authorized. ForceUnauth forces the port to become Unauthorized.

QuietPeriod: Shows the time interval between authentication failure and the start of a new authentication attempt.

TxPeriod: Shows the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.

SuppTimeout: Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.

ServerTimeout: Shows the length of time to wait for a response from a RADIUS server.

MaxReq: Shows the maximum number of times to retry sending packets to the supplicant.

ReAuthPeriod: Shows the time interval between successive reauthentications.

ReAuthenticate: true/false − Shows whether or not to reauthenticate.

show 802.1x auth_configuration	
Syntax	**show 802.1x auth_configuration {ports <portlist>}**
Parameter	*ports <portlist>* − A port or range of ports whose settings are to be displayed.

config 802.1x auth_parameter ports

The **config 802.1x auth_parameter ports** command configures the 802.1x authentication parameters on a range of ports. The default parameter returns all ports in the specified range to their default 802.1x settings.

config 802.1x auth_parameter ports	
Syntax	**config 802.1x auth_parameter ports [<portlist> | all] [default | { port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 300-4294967295> | direction [both | in] | enable_reauth [enable | disable]}]**
Parameter	*<portlist>* – A port or range of ports to be configured. *all* – Specifies all of the ports on the Switch. *default* – Returns all of the ports in the specified range to their 802.1x default settings. *port_control* – Configures the administrative control over the authentication process for the range of ports. The options are: • *force_auth* – Forces the Authenticator for the port to become authorized. Network access is allowed. • *auto* – Allows the port's status to reflect the outcome of the authentication process. • *force_unauth* – Forces the Authenticator for the port to become unauthorized. Network access is blocked. *quiet_period <sec 0-65535>* – Configures the time interval between authentication failure and the start of a new authentication attempt. *tx_period <sec 1-65535>* - Configures the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets. *supp_timeout <sec 1-65535>* - Configures the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets. *server_timeout <sec 1-65535>* - Configures the length of time to wait for a response from a RADIUS server. *max_req <value 1-10>* – Configures the number of times to retry sending packets to a supplicant (user). *reauth_period <sec 300-4294967295>* – Configures the time interval between successive re-authentications. *enable_reauth [enable | disable]* – Determines whether or not the Switch will re-authenticate. Enabled causes re-authentication of users at the time interval specified in the Re-authentication Period field, above. *direction [both | in]* – Sets the administrative-controlled direction to *Both*. If *Both* is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field. The *In* option is not supported in the present firmware release.

config 802.1x init

The **config 802.1x init** command initializes the 802.1x functions on a specified range of ports or for specified MAC addresses operating from a specified range of ports.

config 802.1x init

Syntax	**config 802.1x init port_based ports [<portlist> | all]**
Parameter	*port_based* – Instructs the Switch to initialize 802.1x functions based only on the port number. Ports approved for initialization can then be specified. *ports <portlist>* – A port or range of ports to be configured. *all* – Specifies all of the ports on the Switch.

config 802.1x auth_protocol

The **config 802.1x auth_protocol** command enables configuration of the authentication protocol.

config 802.1x auth_protocol	
Syntax	**config 802.1x auth_protocol [radius_eap | local]**
Parameter	*radius_eap* – Uses the list of RADIUS servers for authentication. *local* – Uses local authentication.

config 802.1x reauth

The **config 802.1x reauth** command re-authenticates a previously authenticated device based on port number.

config 802.1x reauth	
Syntax	**config 802.1x reauth port_based ports [<portlist> | all]**
Parameter	*port_based* – Instructs the Switch to re-authorize 802.1x functions based only on the port number. Ports approved for re-authorization can then be specified. *ports <portlist>* – A port or range of ports to be re-authorized. *all* – Specifies all of the ports on the Switch.

config radius add

The **config radius add** command configures the settings the Switch uses to communicate with a RADIUS server.

config radius add	
Syntax	**config radius add [<server_index 1-3>][<server_ip>] [key <passwd 32>] [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | retransmit <int 1-255>}]**
Parameter	*<server_index 1-3>* – The index of the RADIUS server. *<server_ip>* – The IP address of the RADIUS server. *key* – Specifies that a password and encryption key are to be used between the Switch and the RADIUS server. *<passwd 32>* – The shared-secret key used by the RADIUS server and the Switch. Up to 128 characters can be used. *default* – Uses the default udp port number in both the *auth_port* and *acct_port* settings. *auth_port <udp_port_number 1-65535>* – The UDP port number for authentication requests. The default is 1812. *acct_port <udp_port_number 1-65535>* – The UDP port number for accounting requests. The default is 1813. *retransmit <int 1-255>* –The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 10.

config radius delete

The **config radius delete** command deletes the settings the Switch uses to communicate with a RADIUS server.

config radius delete	
Syntax	**config radius delete [<server_index 1-3>]**
Parameter	*<server_index 1-3>* – The index of the RADIUS server.

config radius

The **config radius** command configures the Switch's RADIUS settings.

config radius	
Syntax	**config radius <server_index 1-3> {key <passwd 32> | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | ipaddress <server_ip> | retransmit <int 1-255> | timeout <int 1-255>}**
Parameter	*<server_index 1-3>* – The index of the RADIUS server. *<server_ip>* – The IP address of the RADIUS server. *key* – Specifies that a password and encryption key are to be used between the Switch and the RADIUS server. • *<passwd 32>* – The shared-secret key used by the RADIUS server and the Switch. Up to 128 characters can be used. *auth_port <udp_port_number 1-65535>* – The UDP port number for authentication requests. The default is 1812. *acct_port <udp_port_number 1-65535>* – The UDP port number for accounting requests. The default is 1813. *retransmit <int 1-255>* – The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255. *timeout <int 1-255>* – Specifies the connection timeout. The value may be between 1 and 255 seconds.

show radius

The **show radius** command displays the current RADIUS configurations on the Switch.

show radius	
Syntax	**show radius**
Parameter	None.

config 802.1x auth_mode

The **config 802.1x auth_mode** command enables either the port-based or MAC-based 802.1x authentication feature on the Switch.

config 802.1x auth_mode	
Syntax	**config 802.1x auth_mode [port_based | mac_based]**
Parameter	*[port_based* | *mac_based]* – Specifies whether 802.1x authentication is by port or MAC address.

create 802.1x user

The **create 802.1x user** command enables network access to a 802.1x user.

create 802.1x user	
Syntax	**create 802.1x user <username 15>**

Parameter	<*vlanname 15*> − The name of the 802.1x user to be created.

delete 802.1x user

The **delete 802.1x user** command deletes network access to a 802.1x user.

delete 802.1x user	
Syntax	**delete 802.1x user <username 15>**
Parameter	<*vlanname 15*> − The name of the 802.1x user to be deleted.

show 802.1x user

The **show 802.1x user** command displays the 802.1x user information.

show 802.1x user	
Syntax	**show 802.1x user <username 15>**
Parameter	<*vlanname 15*> − The name of the 802.1x user to be displayed.

create 802.1x guest_vlan

The **create 802.1x guest_vlan** command enables network access to a 802.1x Guest VLAN. A network administrator can use 802.1x Guest VLANs to deny network access via port–based authentication, but grant Internet access to unauthorized users.

create 802.1x auth_mode	
Syntax	**create 802.1x guest vlan <vlan_name 32>**
Parameter	<*vlan_name 32*> − The name of the 802.1x Guest VLAN to be created.

delete 802.1x guest_vlan

The **delete 802.1x guest_vlan** command disables network access to a 802.1x Guest VLAN. A network administrator can use 802.1x Guest VLANs to deny network access via port–based authentication, but grant Internet access to unauthorized users.

delete 802.1x auth_mode	
Syntax	**delete 802.1x guest vlan <vlan_name 32>**
Parameter	<*vlan_name 32*> − The name of the 802.1x Guest VLAN to be created.

config 802.1x guest_vlan ports

The **config 802.1x guest_vlan ports** command defines a port or range of ports to be members of the 802.1x Guest VLAN. The 802.1x Guest VLAN can be be configured to provide limited network access to authorized member ports. If a member port is denied network access via port–based authorization, but the 802.1x Guest VLAN is enabled, the member port receives limited network access. For example, a network administrator can use the 802.1x Guest VLAN to deny internal network access via port–based authentication, but grant Internet access to unauthorized users.

config 802.1x guest_vlan ports	
Syntax	**config 802.1x guest_vlan ports <portlist> state [enable | disable]**
Parameter	<*portlist*> – A port or range of ports to be configured to the Guest VLAN. *state [enable* | *disable]* – Specifies the guest vlan port is enabled or disabled of the switch.

show 802.1x guest_vlan

The **show 802.1x guest_vlan** command displays the Guest VLAN name, state, and member ports.

show 802.1x guest_vlan	
Syntax	**show 802.1x guest_vlan**
Parameter	None.

24 PORT SECURITY Commands

The Port Security commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config port_security	[<portlist> | all] {admin_state [enable | disable] | max_learning_addr <max_lock_no 0-64> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset] }
show port_security	{<portlist> | all}

Each command is listed in detail, as follows:

config port_security

The **config port_security** command configures port security settings for specific ports.

config port_security	
Syntax	**config port_security [<portlist> | all] {admin_state [enable | disable] | max_learning_addr <max_lock_no 0-64> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset] }**
Parameter	*<portlist>* – A port or range of ports to be configured. *all* – Configures port security for all ports on the Switch. *admin_state [enable* | *disable]* – Enables or disables port security for the listed ports. *max_learning_addr <max_lock_no 0-64>* - 0-64 Limits the number of MAC addresses dynamically listed in the FDB for the ports. *lock_address_mode – Defines the TBD and contains the following options:* • *Permenant* – Learns up to the maximum number of dynamic addresses allowed on the port. The learned addresses are not aged out or relearned on other port for as long as the port is locked. • *DeleteOnReset* – Deletes the current dynamic MAC addresses associated with the port. Learn up to the maximum addresses allowed on the port (this number is also configurable). Aging is disabled; the addresses are deleted on reset. • *DeleteOnTimeout* – Deletes the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Re-learned MAC addresses and address aging out are also enabled. The MAC addresses are deleted when the device is reset and on when the address is aged out.

show port_security

The **show port_security** command displays port security information for the Switch's ports. The information displayed includes port security, admin state, maximum number of learning address and lock mode and trap interval.

config 802.1x guest_vlan	
Syntax	**show port_security {<portlist> | all}**
Parameter	*<portlist>* – A port or range of ports to be displayed. *all* – Displays port security for all ports on the Switch..

25 *TIME AND SNTP Commands*

The Time and SNTP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config sntp	{primary <ipaddr> | secondary <ipaddr> | poll-interval <sec 30-99999>}
show sntp	
enable sntp	
disable sntp	
config time date	<date> <systime>
config time_zone	operator [+ hour <gmt_hour 0-13> minute <minute 0-59> | - hour <gmt_hour 0-12> minute <minute 0-59>]
config dst	[disable | annual [s_date <start_date 1-31> s_mth <start_mth 1-12> s_time <start_time> end_date <integer 1-31> e_mth <end_mth 1-12> e_time <end_time> offset [30 | 60 | 90 | 120]]
show time	

Each command is listed in detail, as follows:

config sntp

The **config sntp** command configures SNTP service from an SNTP server. SNTP must be enabled for this command to function (See **enable sntp**).

config sntp	
Syntax	**config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <sec 30-99999>}**
Parameter	*primary <ipaddr>* – Specifies the IP address of the primary SNTP server. For example, 10.90.90.99. *secondary <ipaddr>* – Specifies the IP address of the secondary SNTP server. *poll-interval <sec 30-99999>* – The interval between requests for updated SNTP information. The polling interval ranges from 30 seconds to 99999 seconds.

show sntp

The **show sntp** command displays SNTP settings information, including the source IP address, time source and poll interval.

show sntp	
Syntax	**show sntp**
Parameter	None.

enable sntp

The **enable sntp** command enables SNTP server support. SNTP service must be separately configured (see **config sntp**). Enabling and configuring SNTP support override any manually configured system time settings.

enable sntp	
Syntax	**enable sntp**
Parameter	None.

disable sntp

The **disable sntp** command disables SNTP support.

disable sntp	
Syntax	**disable sntp**
Parameter	None.

config time date

The **config time date** command configures the system time and date settings. These will be overridden if SNTP is configured and enabled.

config time date	
Syntax	**config time date <date> <systime>**
Parameter	*<date>* – Specifies the date, using two numerical characters for the day of the month, two numerical characters for the name of the month, and four numerical characters for the year. For example: 03082008. *<systime>* – Specifies the system time, using the format hh:mm:ss; that is, two numerical characters each for the hour using a 24-hour clock, the minute and second. For example: 19:42:30.

config time_zone

The **config time_zone** command adjusts the system clock settings according to the time zone. Time zone settings adjust SNTP information accordingly.

config time_zone	
Syntax	**config time_zone operator [+ hour <gmt_hour 0-13> minute <minute 0-59> | - hour <gmt_hour 0-12> minute <minute 0-59>]**
Parameter	*operator* – May be (+) to add or (-) to subtract time to adjust for time zone relative to GMT. *hour <gmt_hour 0-13>* – Specifies the number of hours difference from GMT. *minute <minute 0-59>* – Specifies the number of minutes added or subtracted to adjust the time zone.

config dst

The **config dst** command disables or configures Daylight Saving Time (DST). When enabled, this adjusts the system clock to comply with any DST requirement. DST adjustment affects system time for both manually configured time and time set using SNTP service.

config dst	
Syntax	**config dst [disable | annual [s_date <start_date 1-31> s_mth <start_mth 1-12> s_time <start_time> end_date <integer 1-31> e_mth <end_mth 1-12> e_time <end_time> offset [30 | 60 | 90 | 120]]**
Parameter	*disable* - Disables the DST seasonal time adjustment for the Switch. *annual* - Enables DST seasonal time adjustment on an annual basis. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14. The format for annual mode is as follows, and in the order listed: • *s_date<start_date 1-31>* - The day of the month to begin DST, expressed numerically**.** • *s_mth<start_mth 1-12>* - The month of the year to begin DST, expressed numerically. • *s_time<starttime>* - The time of day to begin DST in hours and

minutes, expressed using a 24-hour clock.

- *end_date<integer 1-31>* - The day of the month to end DST, expressed numerically**.**
- *e_mth<end_mth 1-12>* - The month of the year to end DST, expressed numerically.
- *e_time<end_time>* - The time of day to end DST, in hours and minutes, expressed using a 24-hour clock.

offset [30 | 60 | 90 | 120] - Indicates the number of minutes to add during the summertime. The possible offset times are 30, 60, 90, and 120. The default value is 60.

show time

The **show time** command displays the system time and date configuration, as well as displays the current system time.

show time	
Syntax	**show time**
Parameter	None.

26 *ARP SPOOFING Commands*

The ARP Spoofing commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create ArpSpoofing	[ip_address <ip_addr> mac_address <mac_addr>]
delete ArpSpoofing	[ip_address <ip_addr>]
show ArpSpoofing	
config arp_aging time	<value 0-65535>
clear arptable	

Each command is listed in detail, as follows:

create ArpSpoofing

The **create ArpSpoofing** command enters an IP address and the corresponding MAC address into the Switch's ARP table.

create ArpSpoofing	
Syntax	**create ArpSpoofing [ip_address <ip_addr> mac_address <mac_addr>]**
Parameter	*ip_address <ip_addr>* − Specifies the IP address of the end node or station. *mac_address<mac_addr>* − Specifies the MAC address corresponding to the IP address above.

delete ArpSpoofing

The **delete ArpSpoofing** command deletes an IP address and the corresponding MAC address into the Switch's ARP table.

delete ArpSpoofing	
Syntax	**delete ArpSpoofing [ip_address <ip_addr>]**
Parameter	*ip_address <ip_addr>* − The IP address of the end node or station.

show ArpSpoofing

The **show ArpSpoofing** command displays the IP address and the corresponding MAC address of the Switch's ARP table.

show ArpSpoofing	
Syntax	**show ArpSpoofing**
Parameter	None.

config arp_aging time

The **config arp_aging time** command sets the maximum amount of time, in minutes, that an ARP entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table.

config arp_aging time	
Syntax	**config arp_aging time <value 0-65535>**
Parameter	*time <value 0-65535>* – The ARP age-out time, in minutes. The value may be in the range of 0-65535 minutes, with a default setting of 20

minutes.

clear arptable

The **clear arptable** command is used to remove dynamic ARP table entries from the Switch's ARP table. Static ARP table entries are not affected.

clear arptable	
Syntax	**clear arptable**
Parameter	None.

27 COMMAND HISTORY LIST Commands

The Command History List commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
?	
show command_history	
dir	
config command_history	<value 1-40>

Each command is listed in detail, as follows:

?

The **?** command displays all of the commands available through the Command Line Interface (CLI).

?	
Syntax	**?**
Parameter	*{<command>}* – Lists all the corresponding parameters for the specified command, along with a brief description of the command's function and similar commands having the same words in the command.

show command_history

The **show command_history** command displays the command history.

show command_history	
Syntax	**show command_history**
Parameter	None.

dir

The **dir** command displays all commands.

dir	
Syntax	**dir**
Parameter	None.

config command_history

The **config command_history** command configures the command history.

config command_history	
Syntax	**config command_history <value 1-40>**
Parameter	*<value 1-40>* – The number of previously executed commands maintained in the buffer. Up to 40 of the latest executed commands may be viewed.

28 SSH Commands

The SSH commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable ssh	
disable ssh	
config ssh user	<string 15> authmode [hostabsed | password | publickey]
config ssh authmode	[hostbased | password | publickey] [enable | disable]
show ssh authmode	
config ssh server	{authfail <int 2-20> | contimeout <sec 120-600> | maxsession <int 1-4>| rekey [10min | 30min | 60min | never]}
show ssh server	
config ssh algorithm	[3DES | DES | MD5 | RSA | SHA1] [disable | enable]
show ssh algorithm	
show ssh user authmode	

Each command is listed in detail, as follows:

enable ssh

The **enable ssh** command enables SSH on the Switch.

enable ssh	
Syntax	**enable ssh**
Parameter	None.

disable ssh

The **disable ssh** command disables SSH on the Switch.

disable ssh	
Syntax	**disable ssh**
Parameter	None.

config ssh user

The **config ssh user** command configures the SSH authentication mode for users attempting to access the Switch.

config ssh user	
Syntax	**config ssh user <string 15> authmode [hostabsed | password | publickey]**
Parameter	*<string 15>* – Specifies the name of SSH user. *[hostabsed* | *password* | *publickey]* – Specifies which configuration will be set on a SSH server for authentication.

config ssh authmode

The **config ssh authmode** command configures the SSH authentication mode for users attempting to access the Switch.

config ssh authmode

Syntax	**config ssh authmode [hostbased | password | publickey] [enable | disable]**
Parameter	*[hostabsed* | *password* | *publickey]* – Specifies which configuration will be set on a SSH server for authentication. *[enable* | *disable]* – Specifies that a hostbased, password or publickey configuration set on a SSH server is to be used for authentication.Enables or disables SSH authentication on the Switch.

show ssh authmode

The **show ssh authmode** command displays the current SSH authentication set on the Switch.

show ssh authmode	
Syntax	**show ssh authmode**
Parameter	None.

config ssh server

The **config ssh server** command configures the SSH server.

config ssh server	
Syntax	**config ssh server {authfail <int 2-20> | contimeout <sec 120-600> | maxsession <int 1-4>| rekey [10min | 30min | 60min | never]}**
Parameter	*authfail <int 2-20>* – Specifies the authfail times. The value may be between 2 and 20 times. *timeout <sec 120-600>* – Specifies the connection timeout. The value may be between 120 and 600 seconds. The default is 600 seconds. *maxsession <int 1-4>* – Specifies the maxseeion of ssh server. rekey [10min | 30min | 60min | never] – Specifies the rekey time. The possible values are 10min, 30min, 60min and never.

show ssh server

The **show ssh server** command displays the current SSH sever settings on the Switch.

show ssh server	
Syntax	**show ssh server**
Parameter	None.

config ssh algorithm

The **config ssh algorithm** command configures the SSH algorithm setting on the Switch.

config ssh algorithm	
Syntax	**config ssh algorithm [3DES | DES | MD5 | RSA | SHA1] [disable | enable]**
Parameter	Select the algorithm to be disabled or enabled: ▪ *3DES* – Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. ▪ *DES* – Data Encryption Standard encryption algorithm with Cipher Block Chaining. ▪ *MD5* – Hash for Message Authentication Code (HMAC) MD5 Message Digest (MD5) mechanism. ▪ *RSA* – Hash for Message Authentication Code (HMAC) mechanism utilizing the RSA encryption algorithm. ▪ *SHA1* – Hash for Message Authentication Code (HMAC)

Secure Hash Algorithm (SHA) mechanism.

[disable | eanble] – Enables or Disables the SSH algorithm on the Switch.

show ssh algorithm

The **show ssh algorithm** command displays the current SSH algorithm setting status.

show ssh algorithm	
Syntax	**show ssh algorithm**
Parameter	None.

show ssh user authmode

The **show ssh user authmode** command displays the current SSH user authentication mode setting status.

show ssh user authmode	
Syntax	**show ssh user authmode**
Parameter	None.

29 SSL Commands

The SSL commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable ssl	{ciphersuite {DH-RSA-3DES-SHA1 | DH-RSA-DES-SHA1 | RSA-3DES-SHA1 | RSA-DES-SHA1 | RSA-EXP1024-DES-SHA1 | RSA-NULL-MD5 | RSA-NULL_SHA1}}
disable ssl	{ciphersuite {DH-RSA-3DES-SHA1 | DH-RSA-DES-SHA1 | RSA-3DES-SHA1 | RSA-DES-SHA1 | RSA-EXP1024-DES-SHA1 | RSA-NULL-MD5 | RSA-NULL_SHA1}}
download ssl	certificate <ipaddr> certfilename <path_filename 64>
show ssl	

Each command is listed in detail, as follows:

enable ssl

The **enable ssl** command enables SSL on the Switch by implementing every combination of listed ciphersuites on the Switch. Entering this command enables the SSL status on the Switch. Enabling SSL disables the web-manager on the Switch.

enable ssl	
Syntax	**enable ssl {ciphersuite {DH-RSA-3DES-SHA1 | DH-RSA-DES-SHA1 | RSA-3DES-SHA1 | RSA-DES-SHA1 | RSA-EXP1024-DES-SHA1 | RSA-NULL-MD5 | RSA-NULL_SHA1}}**
Parameter	*ciphersuite – Specifies a cipher suite combination to be enabled.* ▪ *DH-RSA-3DES-SHA1* – Indicate DH key exchange with 3DES encryption and SHA hash. ▪ *DH-RSA-DES-SHA1* – Indicate DH key exchange with DES encryption and SHA hash. ▪ *RSA-3DES-SHA1* – Indicate RSA key exchange with 3DES encryption and SHA hash. ▪ *RSA-DES-SHA1* – Indicate RSA key exchange with DES encryption and SHA hash. ▪ *RSA-EXP1024-DES-SHA1* – Indicate RSA key exchange with EXP1024-DES encryption and SHA hash. ▪ *RSA-NULL-MD5* – Indicate RSA key exchange with NULL encryption and MD5 hash. ▪ *RSA-NULL_SHA1* – Indicate RSA key exchange with NULL encryption and SHA hash.

disable ssl

The **disable ssl** command disables SSL on the Switch and can be used to disable all combinations of listed ciphersuites on the Switch.

disable ssl	
Syntax	**disable ssl {ciphersuite {DH-RSA-3DES-SHA1 | DH-RSA-DES-SHA1 | RSA-3DES-SHA1 | RSA-DES-SHA1 | RSA-EXP1024-DES-SHA1 | RSA-NULL-MD5 | RSA-NULL_SHA1}}**
Parameter	ciphersuite – Specifies a cipher suite combination to be disabled. ▪ *DH-RSA-3DES-SHA1* – Indicate DH key exchange with 3DES encryption and SHA hash. ▪ *DH-RSA-DES-SHA1* – Indicate DH key exchange with DES

encryption and SHA hash.

- *RSA-3DES-SHA1* – Indicate RSA key exchange with 3DES encryption and SHA hash.
- *RSA-DES-SHA1* – Indicate RSA key exchange with DES encryption and SHA hash.
- *RSA-EXP1024-DES-SHA1* – Indicate RSA key exchange with EXP1024-DES encryption and SHA hash.
- *RSA-NULL-MD5* – Indicate RSA key exchange with NULL encryption and MD5 hash.
- *RSA-NULL_SHA1* – Indicate RSA key exchange with NULL encryption and SHA hash.

download ssl

The **download ssl** command displays the SSL status and the certificate file status on the Switch.

download ssl	
Syntax	**download ssl certificate <ipaddr> certfilename <path_filename 64>**
Parameter	*<ipaddr>* – Specifies the IP address of SSL file. *<path_filename 64>* –The DOS path and filename of the SSL file, up to 64 characters, on the TFTP server. For example, C:\31xx.had.

show ssl

The **show ssl** command displays the SSL status and the certificate file status on the Switch.

show ssl	
Syntax	**show ssl**
Parameter	None.

30 ACCESS AUTHENTICATION CONTROL Commands

The Access Authentication Control commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create authen_login method_list_name	<string 15>
config authen_login	[default | method_list_name <string 15>] method {tacacs+ | radius | local | none | server_group}
delete authen_login method_list_name	<string 15>
show authen_login	{all | default | method_list_name <string 15>}
create authen_enable method_list_name	<string 15>
config authen_enable	[default | method_list_name <string 15>] method {tacacs+ | radius | local | none | server_group}
delete authen_enable method_list_name	<string 15>
show authen_enable	[all | default | method_list_name <string 15>]
config authen application	{telnet | ssh | all | http] [login | enable] [default | method_list_name <string 15>]
show authen application	
reate authen server_host	c <ip_addr> protocol [radius | tacacs+] {port <integer 1-65535> | key [<key_string 254> | none] | timeout <integer 1-255> | retransmit <integer 1-255>}
config authen server_host	<ip_addr> protocol [radius | tacacs+] {port <integer 1-65535> | key [<key_string 254> | none] | timeout <integer 1-255> | retransmit <integer 1-255>}
delete authen server_host	<ip_addr> protocol [tacacs+ | radius]
show authen server_host	
create authen server_group	<string 15>
config authen server_group	<string 15> [add | delete] server_host <ip_addr> protocol [radius | tacacs+]
delete authen server_group	<string 15>
show authen server_group	
config authen parameter	[attempt <integer 1-255> | response_timout] <integer 0-255>
show authen parameter	
enable admin	
config admin local_enable	

Each command is listed in detail, as follows:

create authen_login method_list_name

The **create authen_login method_list_name** command creates a list of authentication techniques for user login. The Switch can support up to eight method lists, but one is reserved as a default and cannot be deleted. Multiple method lists must be created and configured separately.

create authen_login method_list_name	
Syntax	**create authen_login method_list_name <string 15>**
Parameter	<*string 15*> - Defines the *method_list_name* to be created as a string of up to 15 alphanumeric characters.

config authen_login

The **config authen_login** command configures a user-defined or default *method list* of authentication methods for users logging on to the Switch. The sequence of methods implemented in this command affects the authentication result. For example, if a user enters a sequence of methods like *tacacs – local,* the Switch sends an authentication request to the first *tacacs* host in the server group. If no response comes from the server host, the Switch sends an authentication request to the second *tacacs* host in the server group and so on, until the list is exhausted. When the local method is used, the privilege level is dependant on the local account privilege configured on the Switch.

Successful login using any of these methods gives the user a 'user' priviledge only. If the user wishes to upgrade his or her status to the administrator level, the user must implement the *enable admin* command, followed by a previously configured password. (*See the **enable admin** part of this section for more detailed information, concerning the **enable admin** command.)*.

create authen_login	
Syntax	**config authen_login [default | method_list_name <string 15>] method {tacacs+ | radius | local | none | server_group}**
Parameter	*default* – The default method list for access authentication, as defined by the user. The user may choose one or more of the following authentication methods: ▪ *tacacs+* – Specifies that the user is to be authenticated using the *TACACS+* protocol from the remote TACACS+ *server hosts* of the TACACS+ *server group* list. ▪ *radius* - Specifies that the user is to be authenticated using the *RADIUS* protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list. ▪ *local* - Specifies that the user is to be authenticated using the local *user account* database on the Switch. ▪ *none* – Specifies that no authentication is required to access the Switch. ▪ *server_group* –Specifies that the user is to be authenticated using the server group *account* database on the Switch. *method_list_name* <*string 15*> – Specifies a previously created method list name defined by the user. One or more of the following authentication methods may be added to this method list: ▪ *tacacs+* – Specifies that the user is to be authenticated using the *TACACS+* protocol from a remote TACACS+ server. ▪ *radius* - Specifies that the user is to be authenticated using the *RADIUS* protocol from a remote RADIUS server. ▪ *local* - Specifies that the user is to be authenticated using the local *user account* database on the Switch. ▪ *none* – Specifies that no authentication is required to access the Switch. ▪ *server_group* –Specifies that the user is to be authenticated using the server group account database on the Switch.

delete authen_login method_list_name

The **delete authen_login method_list_name** command deletes a list of authentication methods for user login.

delete authen_login method_list_name	
Syntax	**delete authen_login method_list_name <string 15>**
Parameter	<*string 15*> - Defines the *method_list_name* to be deleted as a string of up to 15 alphanumeric characters.

show authen_login

The **show authen_login** command displays a list of authentication methods for user login.

show authen_login	
Syntax	**show authen_login {all | default | method_list_name <string 15>}**
Parameter	*default* – Displays the default method list for users logging on to the Switch. *method_list_name* <*string 15*> - Specifies the *method_list_name* to display. *all* – Displays all the authentication login methods currently configured on the Switch. The command displays the following parameters: • Method List Name – The name of a previously configured method list name. • Method Name – Defines which security protocols are implemeted, per method list name.

create authen_enable method_list_name

The **create authen_enable method_list_name** command creates a list of authentication methods for promoting users with normal level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight (8) enable method lists can be implemented on the Switch.

create authen_enable method_list_name	
Syntax	**create authen_enable method_list_name <string 15>**
Parameter	<*string 15*> - Defines the *authen_enable method_list_name* to be created as a string of up to 15 alphanumeric characters.

config authen_enable

The **config authen_enable** command configures a user-defined list of authentication methods for promoting normal user level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight (8) enable method lists can be implemented simultaneously on the Switch.

The sequence of methods implemented in this command affects the authentication result. For example, if a user enters a sequence of methods like *tacacs+ – radius – local-server group,* the Switch sends an authentication request to the first *TACACS+* host in the server group. If no verification is found, the Switch sends an authentication request to the second *TACACS+* host in the server group and so on, until the list is exhausted. At that point, the Switch restarts the same sequence with the following protocol listed, *radius*. If no authentication takes place using the *radius* list, the *local_enable* password set in the Switch is used to authenticate the user.

Successful authentication using any of these methods gives the user an ‘Admin’ level privilege.

config authen_enable	
Syntax	**config authen_enable [default | method_list_name <string 15>] method {tacacs+ | radius | local | none | server_group}**
Parameter	*default* – The default method list for adminstration rights authentication, as defined by the user. The user may choose one or more of the following authentication methods: • *tacacs+* – Specifies that the user is to be authenticated using the *TACACS+* protocol from the remote TACACS+ *server hosts* of the TACACS+ *server group* list. • *radius* – Specifies that the user is to be authenticated using the *RADIUS* protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list. • *local_enable* – Specifies that the user is to be authenticated using the local *user account* database on the Switch. • *none* – Specifies that no authentication is required to access the Switch. • *server_group* – Specifies that the user is to be authenticated using the server group account database on the Switch. *method_list_name <string 15>* – Specifies a previously created *authen_enable method_list_name*. The user may add one or more of the following authentication methods to this method list: • *tacacs+* – Specifies that the user is to be authenticated using the *TACACS+* protocol from a remote TACACS+ server. • *radius* - Specifies that the user is to be authenticated using the *RADIUS* protocol from a remote RADIUS server. • *local_enable* - Specifies that the user is to be authenticated using the local *user account* database on the Switch. • *none* – Specifies that no authentication is required to access the Switch. • *server_group* – Specifies that the user is to be authenticated using the server group account database on the Switch.

delete authen_enable method_list_name

The **delete authen_enable method_list_name** command deletes a user-defined list of authentication methods for promoting user level privileges to Adminstrator level privileges.

delete authen_enable method_list_name	
Syntax	**delete authen_enable method_list_name <string 15>**
Parameter	*<string 15>* - Defines the *authen_enable method_list_name* to be deleted as a string of up to 15 alphanumeric characters.

show authen_enable

The **show authen_enable** command deletes a user-defined list of authentication methods for promoting user level privileges to Adminstrator level privileges.

show authen_enable	
Syntax	**show authen_enable [all | default | method_list_name <string 15>]**
Parameter	*default* – Displays the default method list for users attempting to gain access to Administrator level privileges on the Switch. *method_list_name <string 15>* – The *method_list_name* to be displayed. *all* – Displays all the authentication login methods currently configured on the Switch. The command displays the following parameters:

- Method List Name – The name of a previously configured method list name.
- Method Name – Defines which security protocols are implemeted, per method list name.

config authen application

The **config authen application** command configures Switch applications (HTTP, Telnet, SSH) for login at the user level and at the administration level (*authen_enable*), utilizing a previously configured method list.

config authen application	
Syntax	**config authen application {telnet | ssh | all | http] [login | enable] [default | method_list_name <string 15>]**
Parameter	*application* – Specifies the application to configure. One of the following four options may be selected: • *telnet* – Configures the Telnet login method. • *ssh* – Configures the Secure Shell login method. • *all* – Configures all applications as (HTTP, Telnet, SSH) login methods. • *http* – Configures the http login method. *login* – Configures an application for normal login on the user level, using a previously configured method list. *enable* – Configures an application for upgrading a normal user level to administrator privileges, using a previously configured method list. *default* – Configures an application for user authentication using the default method list. *method_list_name <string 15>* – Configures an application for user authentication using a previously configured *method_list_name*.

show authen application

The **show authen application** command displays all of the authentication method lists (login, enable administrator privileges) for Switch configuration applications (console, Telnet, SSH) currently configured on the Switch.

show authen application	
Syntax	**show authen application**
Parameter	None.

create authen server_host

The **create authen server_host** command creates an authentication server host for the TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with authentication protocol enabled, the Switch sends authentication packets to a remote TACACS+/RADIUS server host on a remote host. The TACACS+/RADIUS server host then verifies or denies the request and returns the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

create authen server_host	
Syntax	**create authen server_host <ip_addr> protocol [radius | tacacs+] {port <integer 1-65535> | key [<key_string 254> | none] | timeout <integer 1-255> | retransmit <integer 1-255>}**
Parameter	*server_host <ip_addr>* – The IP address of the remote server host to add. *protocol* – The protocol used by the server host. The options are:

- *tacacs+* – Specifies that the server host utilizes the TACACS+ protocol.
- *radius* – Specifies that the server host utilizes the RADIUS protocol.

port <integer 1-65535> – The virtual port number of the authentication protocol on a server host. The value must be between 1 and 65535. The default port number is 49 for TACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security.
key [<key_string 254> | none] – The authentication key to be shared with a configured TACACS+ or RADIUS server only. The value is a string of up to 254 alphanumeric characters, or *none*.
timeout <integer 1-255> – The time in seconds the Switch waits for the server host to reply to an authentication request. The default value is 5 seconds.

retransmit <integer 1-255> – The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255. This field is inoperable for the TACACS+ protocol.

config authen server_host

The **config authen server_host** command configures a user-defined authentication server host for the TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with the authentication protocol enabled, the Switch sends authentication packets to a remote TACACS+/RADIUS server host on a remote host. The TACACS+/RADIUS server host then verifies or denies the request and returns the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

config authen server_host	
Syntax	**config authen server_host <ip_addr> protocol [radius | tacacs+] {port <integer 1-65535> | key [<key_string 254> | none] | timeout <integer 1-255> | retransmit <integer 1-255>}**
Parameter	*server_host <ip_addr>* – The IP address of the remote server host to add. *protocol* – The protocol used by the server host. The options are: • *tacacs+* – Specifies that the server host utilizes the TACACS+ protocol. • *radius* – Specifies that the server host utilizes the RADIUS protocol. *port <integer 1-65535>* – The virtual port number of the authentication protocol on a server host. The value must be between 1 and 65535. The default port number is 49 for TACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security. *key [<key_string 254> | none]* – The authentication key to be shared with a configured TACACS+ or RADIUS server only. The value is a string of up to 254 alphanumeric characters, or *none*. *timeout <integer 1-255>* – The time in seconds the Switch waits for the server host to reply to an authentication request. The default value is 5 seconds. *retransmit <integer 1-255>* –The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255. This field is inoperable for the TACACS+ protocol.

delete authen server_host

The **delete authen server_host** command deletes a user-defined authentication server host previously created on the Switch.

delete authen server_host	
Syntax	**delete authen server_host <ip_addr> protocol [tacacs+ | radius]**
Parameter	*server_host <ip_addr>* - The IP address of the remote server host to be deleted. *protocol* – The protocol used by the server host the user wishes to delete. The options are: • *tacacs+* – Specifies that the server host utilizes the TACACS+ protocol. • *radius* – Specifies that the server host utilizes the RADIUS protocol.

show authen server_host

The **show authen server_host** command displays user-defined authentication server hosts previously created on the Switch.

The following parameters are displayed:

IP Address: The IP address of the authentication server host.

Protocol: The protocol used by the server host. Possible results include TACACS+ or RADIUS.

Port: The virtual port number on the server host. The default value is 49.

Timeout: The time in seconds the Switch waits for the server host to reply to an authentication request.

Retransmit: The value in the retransmit field denotes how many times the device resends an authentication request when the TACACS server does not respond. This field is inoperable for the tacacs+ protocol.

Key: Authentication key to be shared with a configured TACACS+ server only.

show authen server_host	
Syntax	**show authen server_host**
Parameter	None.

create authen server_group

The **create authen server_group** command creates an authentication server group on the Switch.

create authen server_group	
Syntax	**create authen server_group <string 15>**
Parameter	*<string 15>* - Defines the authentication group name as a string of up to 15 alphanumeric characters.

config authen server_group

The **config authen server_group** command provides user to configure the authentication server group on the Switch.

config authen server_group	
Syntax	**config authen server_group <string 15> [add | delete] server_host <ip_addr> protocol [tacacs+ | radius]**
Parameter	*<string 15>* – Defines the authentication group name as a string of up to 15 alphanumeric characters. *[add | delete]* – Specifies the authentication server host will be add or deleted of the server group.

server_host <ip_addr> – The IP address of the remote server host to be deleted.

protocol – The protocol used by the server group the user wishes to delete. The options are:

- *tacacs+* – Specifies that the server host utilizes the TACACS+ protocol.
- *radius* – Specifies that the server group utilizes the RADIUS protocol.

delete authen server_group

The **delete authen server_host** command deletes a user-defined authentication server host previously created on the Switch.

delete authen server_group	
Syntax	**delete authen server_group <string 15>**
Parameter	*<string 15>* – Specifies the authentication server group name to be deleted.

show authen server_group

The **show authen server_host** command displays a user-defined authentication server group previously created on the Switch.

show authen server_group	
Syntax	**show authen server_group**
Parameter	None.

config authen parameter

The **config authen parameter** command provides user to configure the authentication parameters on the Switch.

config authen parameter	
Syntax	**config authen parameter [attempt <integer 1-255> | response_timout] <integer 0-255>**
Parameter	*attemtp <integer 1-255>* – Specifies the attempt of authentication parameter on the Switch. The value range is between 1 and 255. *response_timout <integer 0-255>* – Specifies the response timout of authentication parameter on the Switch. The value range is between 0 and 255.

show authen parameter

The **show authen parameter** command displays the authentication parameter on the Switch.

show authen parameter	
Syntax	**show authen parameter**
Parameter	None.

enable admin

The **enable admin** command enables a user to be granted administrative privileges on to the Switch. After logging on to the Switch, users have only 'user' level privileges. To gain access to administrator level privileges, the user may enter this command. The system then prompts for an authentication password. Possible authentication methods for this function include TACACS, TACACS+, RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (none). Because TACACS does not support the enable function, the user must create a special account on

the server host which has the username ‘enable’, and a password configured by the administrator that will support the ‘enable’ function. This function becomes inoperable when the authentication policy is disabled.

enable admin	
Syntax	**enable admin**
Parameter	None.

config admin local_enable

The **config admin local_enable** command changes the locally enabled password for the **local_enable admin** command. When a user chooses the ‘*local_enable*’ method to promote user level privileges to administrator privileges, the user is prompted to enter the password configured here.

After entering the **config admin local_enable** command, the user is prompted to enter the old password, then a new password in a string of no more than 15 alphanumeric characters, and finally prompted to enter the new password again for confirmation. See the example below.

config admin local_enable	
Syntax	**config admin local_enable**
Parameter	None.

31 *LACP Commands*

The LACP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config lacp port_priority	<portlist> [value 1-65535] [timeout <long | short>]
show lacp	{<portlist>}

Each command is listed in detail, as follows:

config lacp port_priority

The **config lacp port_priority** command sets the LACP priority value and administrative timeout of a physical port or range of ports in an LACP group.

config lacp port_priority	
Syntax	**config lacp port_priority <portlist> [value 1-65535] [timeout <long | short>]**
Parameter	<*portlist*> - A port or range of ports to be configured. <*value 1-65535*> - Specifies the LACP priority value for a port or range of ports to be configured. The default is 1. <*timeout*> - Specifies the administrative LACP timeout. • *long(90sec)* – Specifies the LACP timeout to be 90 seconds. This is the default. • *short(3sec)* – Specifies the LACP timeout to be 3 seconds.

show lacp

The **show lacp** command displays the current LACP mode settings.

show lacp	
Syntax	**show lacp {<portlist>}**
Parameter	<*portlist*> - A port or range of ports to be displayed.

32 *LLDP Commands*

The LLDP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable lldp	
disable lldp	
config lldp ports	[<portlist> | all] admin_status [tx_only | rx_only | tx_and_rx | disable]
config lldp ports	[<portlist> | all] basic_tlvs [port_description | system_name | system_capabilities | system_description | all] [disable | enable]
config lldp ports	[<portlist> | all] dot1_tlv_protocol_identity [eapol | gvrp | lacp | stp | all] [disable | enable]
config lldp ports	[<portlist> | all] dot1_tlv_pvid [disable | enable]
config lldp ports	[<portlist> | all] dot1_tlv_vlan_name [vlan <vlan_name 32> | vlanid <vidlist>][disable | enable]
config lldp ports	[<portlist> | all] dot3_tlvs [{link_aggregation | mac_phy_configuration_status | maximum_frame_size | power_via_mdi} | all][disable | enable]
config lldp ports	[<portlist>|all] mgt_addr [enable | disable]
config lldp ports	[<portlist> | all] notification [enable | disable]
config lldp message_tx_interval	<sec 5-32768>
config lldp message_tx_hold_multiplier	<int 2-10>
config lldp reinit_delay	< sec 1-10>
config lldp tx_delay	< sec 1-8192>
config lldp notification_interval	< sec 5-3600>
show lldp	
show lldp ports	<portlist>
show lldp mgt_addr	{ipv4 <ipaddr>}
show lldp local_ports	{<portlist> | mode[brief | normal | detailed]}
show lldp remote_ports	{<portlist> **|** mode[brief | normal | detailed]}
show lldp statistics	{ports <portlist>}

Each command is listed in detail, as follows:

enable lldp

The **enable lldp** command enables the *Link Layer Discovery Protocol* (LLDP) on the switch.

enable lldp	
Syntax	**enable lldp**
Parameter	None.

disable lldp

The **disable lldp** command disables the *Link Layer Discovery Protocol* (LLDP) on the switch.

disable lldp	
Syntax	**disable lldp**
Parameter	None.

config lldp ports

The **config lldp ports** command defines lldp admin status per port on the switch.

config lldp ports	
Syntax	**config lldp ports [<portlist> | all] admin_status [tx_only | rx_only | tx_and_rx | disable]**
Parameter	*<portlist>* - A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured. *admin status* – Defines admin status of ports on the switch. The possible values are: tx_only, rx_only, tx_and_rx and disable.

config lldp ports

The **config lldp ports** command defines lldp admin status per port on the switch.

config lldp ports	
Syntax	**config lldp ports [<portlist> | all] basic_tlvs [port_description | system_name | system_capabilities | system_description | all] [disable | enable]**
Parameter	*<portlist>* - A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured. Basic TLVs: *port_description* – Advertisement of Port description. system_name – Advertisement of system name. *system capabilities* – Advertisement of system capabilities. *system description* – Advertisement of System description. *all* – Advertisement of all the basic TLVs.

config lldp ports

The **config lldp ports** command defines lldp admin status per port on the switch.

config lldp ports	
Syntax	**config lldp ports [<portlist> | all] dot1_tlv_protocol_identity [eapol | gvrp | lacp | stp | all] [disable | enable]**
Parameter	*<portlist>* − A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured. *dot1_tlv_protocol_identity* − Defines if the advertisement is enabled or disabled. The possible values are: eapol, gvrp, lacp, stp or all.

config lldp ports

The **config lldp ports** dot1_tlv_pvid command defines lldp admin status per port on the switch.

config lldp ports	
Syntax	**config lldp ports [<portlist> | all] dot1_tlv_pvid [disable | enable]**
Parameter	*<portlist>* - A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured. *dot1_tlv_pvid* − Defines if the advertisement is enabled or disabled.

config lldp ports

The **config lldp ports** dot1_tlv_vlan_name command defines lldp admin status per port on the switch.

config lldp ports	
Syntax	**config lldp ports [<portlist> | all] dot1_tlv_vlan_name [vlan <vlan_name 32> | vlanid <vidlist>][disable | enable]**
Parameter	*<portlist>* - A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured. *dot1_tlv_vlan_name* − Defines if the advertisement is enabled or disabled. vlan <vlan_name 32> − The name of the VLAN to be configured. vlanid <vidlist> − The vid of the VLAN to be configured.

config lldp ports

The **config lldp** dot3 TLVs command defines if lldp will advertise the mac_phy_configuration_status the command is per port on the switch.

config lldp ports	
Syntax	**config lldp ports [<portlist> | all] dot3_tlvs [{link_aggregation | mac_phy_configuration_status | maximum_frame_size | power_via_mdi} | all][disable | enable]**
Parameter	*<portlist>* - A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured. dot3_tlvs – defines if the advertisement is enabled or disabled. The possible values are: link_aggregation, mac_phy_configuration_status, maximum_frame_size, power_via_mdi or all.

config lldp ports

The **config lldp** mgt_addr command defines if lldp will advertise the switch's IP address the command is per port on the switch.

config lldp ports	
Syntax	**config lldp ports [<portlist>|all] mgt_addr [enable | disable]**
Parameter	*<portlist>* - A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured. *mgt_addr* – defines wether the management address (IP address) advertisement will be enabled or disabled.

config lldp ports

The **config lldp** ports notification command defines lldp notification per port on the switch.

config lldp ports	
Syntax	**config lldp ports [<portlist> | all] notification [enable | disable]**
Parameter	*<portlist>* - A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured.. *notification [enable* | *disable***]**– defines is notification is enabled or disabled.

config lldp message_tx_interval

The **config lldp message_tx_interval** defines the lldp message interval of the incoming messages.

config lldp message_tx_interval

Syntax	**config lldp message_tx_interval <sec 5-32768>**
Parameter	*<sec 5-32768>l* – Defines the message interval time. The range is between 5 and 32768.

config lldp message_tx_hold_multiplier

The **config lldp message_tx_hold_multiplier** command specifies the amount of time the receiving device should hold a *Link Layer Discovery Protocol* (LLDP) packet before discarding it.

config lldp message_tx_hold_multiplier	
Syntax	**config lldp message_tx_hold_multiplier <int 2-10>**
Parameter	*<int 2-10>* –Specifies the hold time to be sent in the LLDP update packets as a multiple of the timer value. (Range: 2-10). The default configuration is 4.

config lldp reinit_delay

The **config lldp reinit_delay** command specifies the minimum time an LLDP port will wait before reinitializing LLDP transmission.

config lldp reinit_delay	
Syntax	**config lldp reinit_delay < sec 1-10>**
Parameter	*<sec 1-10>* –Specifies the minimum time in seconds an LLDP port will wait before reinitializing LLDP transmission. The range is 1 – 10 seconds. The default configuration is 2 seconds.

config lldp tx_delay

The **lldp tx_delay** command specifies the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB, use the **lldp tx_delay** command in global configuration mode.

config lldp tx_delay	
Syntax	**config lldp tx_delay < sec 1-8192>**
Parameter	*<sec 1-8192>* –Specifies the minimum time in seconds an LLDP TX port will wait before reinitializing LLDP transmission. The range is 1 – 8192 seconds.

config lldp notification_interval

The **config lldp notification_interval** command specifies the notification interval time on an LLDP port.

config lldp notification_interval	
Syntax	**config lldp notification_interval < sec 5-3600>**
Parameter	*<sec 5-3600>* –Specifies the notification interval time in seconds on an LLDP port. The range is 5-3600 seconds.

show lldp

The **show lldp** command displays the information and configuration of the Switch.

show lldp	
Syntax	**show lldp**
Parameter	None.

show lldp ports

The **show lldp ports** command displays the information regarding to the ports.

show lldp ports	
Syntax	**show lldp ports <portlist>**
Parameter	*<portlist>* − A port or range of ports to be displayed.

show lldp mgt_addr

The **show lldp mgt_addr** command displays the information regarding the ipv4 address.

show lldp mgt_addr	
Syntax	**show lldp mgt_addr {ipv4 <ipaddr>}**
Parameter	*ipv4 <ipaddr>* − Specifies the lldp ipv4 address to be displayed.

show lldp local_ports

The **show lldp local_ports** command displays the information regarding neighboring devices.

show lldp local_ports	
Syntax	**show lldp local_ports {<portlist> | mode[brief | normal | detailed]}**
Parameter	*<portlist>* − A port or range of ports to be displayed. *[mode{brief | normal | detailed}]* − defines which mode of information want to be displayed, brief, normal or detailed.

show lldp remote_ports

The **show lldp remote_ports** command displays the information regarding neighboring devices.

show lldp remote_ports	
Syntax	**show lldp remote_ports {<portlist> | mode[brief | normal | detailed]}**
Parameter	*<portlist>* − A port or range of ports to be displayed. *[mode{brief | normal | detailed}]* − defines which mode of information want to be displayed, brief, normal or detailed.

show lldp statistics

The **show lldp statistics** command displays the statistics of lldp on the Switch.

show lldp statistics	
Syntax	**show lldp statistics {ports <portlist>}**
Parameter	*<portlist>* − A port or range of ports to be displayed.

33 IP-MAC-PORT BINDING Commands

The IMPB commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable address_binding arp_mode	
disable address_binding arp_mode	
config address_binding ip_mac	ports [<portlist> | all] [state | allow_zeroip] [enable | disable]

Each command is listed in detail, as follows:

enable address_binding arp_mode

The **enable address_binding arp_mode** command provides user to restrict client access to a switch by enabling administrators to configure pairs of client MAC and IP addresses that are allowed to access networks through a switch.

enable address_binding arp_mode	
Syntax	**enable address_binding arp_mode**
Parameter	None.

disable address_binding arp_mode

The **disable address_binding arp_mode** command disables the IMPB on the Switch.

disable address_binding arp_mode	
Syntax	**disable address_binding arp_mode**
Parameter	None.

config address_binding ip_mac

The **config address_binding ip_mac** command disables the IMPB on the Switch.

config address_binding ip_mac	
Syntax	**config address_binding ip_mac ports [<portlist> | all] [state | allow_zeroip] [enable | disable]**
Parameter	*<portlist>* – A port or range of ports to be configured. *all* – Specifies all ports to be configured. *[state | allow_zeroip]* – Specifies the mode of IMPB ports on the Switch. *[enable | disable]* – Specifies the state or allow_zeroip to be enabled or disabled on the specified ports on the Switch.

34 ACCESS CONTROL LIST Commands

The Access Control List commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create access_profile (For Ethernet)	profile_id <value 1-50> [ethernet {vlan | source_mac <macmask 000000000000-ffffffffffff > |destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}]
create access_profile (For IP)	profile_id <value 1-50> [ip [icmp { type | code } | igmp { type } | tcp { src_port_mask < hex 0x0–0xffff > | dst_port_msk <hex 0x0-0xffff> | flag_mask }} | udp { src_port_mask < hex 0x0–0xffff > | dst_port_msk <hex 0x0-0xffff> }] { source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp }]
config access_profile (For Ethernet)	profile_id <value 1-50> [add | delete] access_id [auto_assign | <value 1-65535>] [ethernet {vlan <vlanid 1-4094> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x5dd-0xffff>} ports <portlist> [mirror | replace_dscp_with <value 0-63> | rx_rate <value 64-1024000>} | deny]
config access_profile (For IP)	profile_id <value 1-50> [add | delete] access_id [auto assign | <value 1-65535>] [ip {source_ip <ipaddr> | protocol_id <value 0-255> | destination_ip <ipaddr> | dscp <value 0–63> | [icmp {type <value 0-255> code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> | dst_port <value 0-65535> |flag {+ | –} {urg | ack | psh | rst | syn | fin } | udp {src_port <value 0-65535> | dst_port <value 0-65535>}]} ports <portlist> [permit {mirror | replace_dscp_with <value 0-63> | rx_rate <value 64-1024000>} | deny]
config access_profile	profile_id <value 1-50> delete access_id <value 1-65535>
delete access_profile	profile_id <value 1-50>
show access_profile	profile_id <value 1-50>
create cpu access_profile (For Ethernet)	profile_id <value 1-3> [ethernet {vlan | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}]
create cpu access_profile (For IP)	profile_id <value 1-3> [ip [icmp { type | code } | igmp { type } | tcp { src_port_mask < hex 0x0–0xffff > | dst_port_msk <hex 0x0-0xffff> | flag_mask }} | udp { src_port_mask < hex 0x0–0xffff > | dst_port_msk <hex 0x0-0xffff> }] { source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp }]
config cpu access_profile (For Ethernet)	profile_id <value 1-3> [add | delete] access_id [<value 1-5> | auto_assign] ethernet [{802.1p <vlue 0-7> | destination_mac <macaddr> | ethernet_type <hex 0x5dd-0xffff> | ports <portlist> | source_mac <macaddr> | vlan <vlanid 1-4094>}]
config cpu access_profile (For IP)	profile_id <value 1-3> [add | delete] access_id [<value 1-5> | auto_assign] IP [{destination_ip <ip_addr> | dscp <value 0-63> | icmp [code <value 0-255>| type <value 0-255>] | igmp type <value 0-255> | ports <portlist> | protocol_id <value 0-255> | source_ip <ip_addr> | tcp[dst_port <value 0-65535> | flag<string> | src_port<value 0-65535>] | udp[dst_port<value 0-65535> | src_port<value 0-65535>]}]
delete cpu access_profile	profile_id <value 1-3>
show cpu access_profile	{profile_id <value 1-3>}

Each command is listed in detail, as follows:

create access_profile (For Ethernet)

The **create access_profile** command creates a profile for packets that may be accepted or denied by the Switch by examining the Ethernet part of the packet header. Specific values for rules pertaining to the Ethernet part of the packet header may be defined by configuring the **config access_profile** command for Ethernet, as stated below.

create access_profile (For Ethernet)	
Syntax	**create access_profile profile_id <value 1-50> [ethernet {vlan | source_mac <macmask 000000000000-ffffffffffff > |destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}]**
Parameter	*profile_id* <*value 1-50*> – Specifies an index number between 1 and 50 that identifies the access profile being created with this command. *ethernet* - Specifies that the Switch examines the layer 2 part of each packet header with emphasis on one or more of the following: • *vlan* – Specifies that the Switch examine the VLAN part of each packet header. • *source_mac* <*macmask 00000000000-fffffffffff*> – Specifies a MAC address mask for the source MAC address. • *destination_mac* <*macmask 00000000000-fffffffffff* > – Specifies a MAC address mask for the destination MAC address. • *802.1p* – Specifies that the Switch examine the 802.1p priority value in the frame's header. • *ethernet_type* – Specifies that the Switch examine the Ethernet type value in each frame's header.

create access_profile (For IP)

The **create access_profile** command creates a profile for packets that may be accepted or denied by the Switch by examining the IP part of the packet header. Specific values for rules pertaining to the IP part of the packet header may be defined by configuring the **config access_profile** command for IP, as stated below.

create access_profile (For IP)	
Syntax	**create access_profile profile_id <value 1-50> [ip [icmp { type | code } | igmp { type } | tcp { src_port_mask < hex 0x0–0xffff > | dst_port_msk <hex 0x0-0xffff> | flag_mask }} | udp { src_port_mask < hex 0x0–0xffff > | dst_port_msk <hex 0x0-0xffff> }] { source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp }]**
Parameter	*profile_id* <*value 1-50*> – Specifies an index number between 1 and 50 that identifies the access profile being created with this command. *ip* - Specifies that the Switch examines the IP fields in each packet with special emphasis on one or more of the following: *icmp* – Specifies that the Switch examines the Protocol field in each frame's IP header , and that the value must be 1 (Internet Control Message Protocol- ICMP) for the action to take place. • *type* – Specifies that the Switch examines each frame's ICMP Type field. • *code* – Specifies that the Switch examines each frame's ICMP Code field. *igmp* – Specifies that the Switch examine each frame's protocol field and it must be 2 (Internet Group Management Protocol-IGMP) for the action to take place. • *type* – Specifies that the Switch examine each frame's IGMP Type field.

tcp – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place.

- *src_port_mask* <*hex 0x0-0xffff*> – Specifies a TCP port mask for the source port.
- *dst_port_mask* <*hex 0x0-0xffff*> – Specifies a TCP port mask for the destination port.
- *flag_mask* – Specifies the appropriate flag_mask parameter.

udp – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place..

- *src_port_mask* <*hex 0x0-0xffff*> – Specifies a UDP port mask for the source port.
- *dst_port_mask* <*hex 0x0-0xffff*> – Specifies a UDP port mask for the destination port.

source_ip_mask <*netmask*> – Specifies an IP address mask for the source IP address.

destination_ip_mask <*netmask*> – Specifies an IP address mask for the destination IP address.

dscp – Specifies that the Switch examines the DiffServ Code Point (DSCP) field in each frame's header.

config access_profile (For Ethernet)

The **config access_profile** command defines the rules used by the Switch to either filter or forward packets based on the Ethernet part of each packet header.

config access_profile (For Ethernet)	
Syntax	**config access_profile profile_id <value 1-50> [add | delete] access_id [auto_assign | <value 1-65535>] [ethernet {vlan <vlanid 1-4094> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x5dd-0xffff>} ports <portlist> [mirror | replace_dscp_with <value 0-63> | rx_rate <value 64-1024000>} | deny]**
Parameter	*profile_id* <*value 1-50*> – Specifies the access profile id to be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The lower the profile ID, the higher the priority the rule will be given. *[add | delete] access_id* <*value 1-65535*> – Adds or deletes an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. Up to 65535 rules may be configured for the Ethernet access profile. • *auto_assign* – Configures the Switch to automatically assign a numerical value (between 1 and 65535) for the rule being configured. *ethernet* – Specifies that the Switch examine only the layer 2 part of each packet to determine if it is to be filtered or forwarded based on one or more of the following: • *vlan* <*vlanid 1-4094*> – Specifies that the access profile applies only to this previously created VLAN. • *source_mac* <*macaddr*> – Specifies that the access profile applies only to packets with this source MAC address. MAC address entries may be made in the following format: 00:00:00:00:00:00-FF:FF:FF:FF:FF:FF • *destination_mac* <*macaddr*> – Specifies that the access

profile applies only to packets with this destination MAC address. MAC address entries may be made in the following format: 00:00:00:00:00:00-FF:FF:FF:FF:FF:FF

- *802.1p <value 0-7>* – Specifies that the access profile applies only to packets with this 802.1p priority value.
- *ethernet_type <hex 0x05dd-0xffff>* – Specifies that the access profile applies only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.

ports <portlist> - The access profile for Ethernet may be defined for each port on the Switch.

- *mirror* – Specifies the action to mirror before being forwarded by the Switch.
- *replace_dscp_with <value 0-63>* – Specifies a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet.
- *rx_rate <value 64-1024000>* – Specifies the rate limit to limit Rx bandwidth for for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate limit of 10 then the ingress rate is 640kbit/sec.) The user many select a value between 64- 1024000 or no limit. The default setting is no limit.

deny – Specifies that packets that do not match the access profile are not permitted to be forwarded by the Switch and will be filtered.

config access_profile (For IP)

The **config access_profile** command defines the rules used by the Switch to either filter or forward packets based on the IP part of each packet header.

config access_profile (For IP)	
Syntax	**config access_profile profile_id <value 1-50> [add | delete] access_id [auto assign | <value 1-65535>] [ip {source_ip <ipaddr> | protocol_id <value 0-255> | destination_ip <ipaddr> | dscp <value 0–63> | [icmp {type <value 0-255> code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> | dst_port <value 0-65535> |flag {+ | –} {urg | ack | psh | rst | syn | fin } | udp {src_port <value 0-65535> | dst_port <value 0-65535>}]} ports <portlist> [permit {mirror | replace_dscp_with <value 0-63> | rx_rate <value 64-1024000>} | deny]**
Parameter	*profile_id <value 1-50>* – Specifies the access profile id to be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The lower the profile ID, the higher the priority the rule will be given. *[add | delete] access_id <value 1-65535>* – Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. Up to 65535 different rules may be configured for the IP access profile. • *auto_assign* – Configures the Switch to automatically assign a numerical value (between 1 and 65535) for the rule being configured. *ip* – Specifies that the Switch examine the IP fields in each packet to determine if it will be either forwarded or filtered based on one or more of the following: • *source_ip <ipaddr>* – Specifies that the access profile applies only to packets with this source IP address. • *protocol_id <value 0-255>* – Specifies that the Switch examine

the Protocol field in each packet and if this field contains the value entered here, apply the appropriate rules.

- *destination_ip <ipaddr>* – Specifies that the access profile applies only to packets with this destination IP address.
- *dscp <value 0-63>* – Specifies that the access profile applies only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header.
- *icmp* – Specifies that the Switch examine the protocol field in each frame's header and it should match Internet Control Message Protocol (ICMP).
- *type* – Specifies that the Switch examine each frame's ICMP Type field.
- *code* – Specifies that the Switch examine each frame's ICMP Code field.
- *igmp* – Specifies that the Switch examine each frame's protocol and it should match Internet Group Management Protocol (IGMP) field.
- *type* – Specifies that the Switch examine each frame's IGMP Type field.
- *tcp* - Specifies that the Switch examine each frame's protocol and it should matchTransport Control Protocol (TCP) field.
- *src_port <value 0-65535>* – Specifies that the access profile applies only to packets that have this TCP source port in their TCP header.
- *dst_port <value 0-65535>* – Specifies that the access profile applies only to packets that have this TCP destination port in their TCP header.
- *flag {+ | –} {urg | ack | psh | rst | syn | fin }}* – Specifies the appropriate flag parameter. All incoming packets have TCP flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets.

  To specify flag bits that should be "1" type + and the flag bit name, to specify bits that should be "0" type – and the flag bit name.
- *udp* – Specifies that the Switch examine the protocol field in each packet and it should match User Datagram Protocol (UDP).
- *src_port <value 0-65535>* – Specifies that the access profile applies only to packets that have this UDP source port in their header.
- *dst_port <value 0-65535>* – Specifies that the access profile applies only to packets that have this UDP destination port in their header.

port [<portlist>| - The access profile for IP may be defined for each port on the Switch.

permit – Specifies that packets that match the access profile are permitted to be forwarded by the Switch.

- *mirror* – Specifies the action to mirror before being forwarded by the Switch.
- *replace_dscp_with <value 0-63>* – Specifies a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet.
- *rx_rate <value 64-1024000>* – Specifies the rate limit to limit

Rx bandwidth for for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate limit of 10 then the ingress rate is 640kbit/sec.) The user many select a value between 64- 1024000 or no limit. The default setting is no limit.

deny – Specifies that packets that do not match the access profile are not permitted to be forwarded by the Switch and will be filtered.

config access_profile

The **config access_profile** command deletes a specific rule from the access profile on the Switch.

config access_profile	
Syntax	**config access_profile profile_id <value 1-50> delete access_id <value 1-65535>**
Parameter	*profile_id <value 1-50>* - Specifies the access profile id that is used to identify the access profile to be configured with this command. *delete access_id <value 1-65535>* – Specifies the specific rule to be deleted from the profile.

delete access_profile

The **delete access_profile** command deletes a previously created access profile on the Switch.

delete access_profile	
Syntax	**delete access_profile profile_id <value 1-50>**
Parameter	*profile_id <value 1-50>* - Specifies the access profile to be deleted.

show access_profile

The **show access_profile** command displays the currently configured access profiles.

show access_profile	
Syntax	**show access_profile profile_id <value 1-50>**
Parameter	*profile_id <value 1-50>* – Specifies the access profile to be displayed. This value is assigned to the access profile when it is created with the **create access_profile** command. If the *profile_id* parameter is omitted, all access profile entries are displayed.

create cpu access_profile (For Ethernet)

The **create cpu access_profile** command is used to create CPU access list rules on the Switch.

create cpu access_profile (For Ethernet)	
Syntax	**create cpu access_profile profile_id <value 1-3> [ethernet {vlan | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}]**
Parameter	*profile_id <value 1-3>* – Specifies the cpu access profile to be displayed. *ethernet* - Specifies that the Switch examines the layer 2 part of each packet header with emphasis on one or more of the following: • *vlan* – Specifies a VLAN mask. • *source_mac <macmask 000000000000-ffffffffffff>* – Specifies the source MAC mask. • *destination_mac <macmask 000000000000-ffffffffffff>* – Specifies the destination MAC mask. • *802.1p* – Specifies 802.1p priority tag mask.

- *ethernet_type* – Specifies the Ethernet type mask.

create cpu access_profile (For IP)

The **create cpu access_profile** command is used to create CPU access list rules on the Switch.

create cpu access_profile (For IP)	
Syntax	**create cpu access_profile profile_id <value 1-3> [ip [icmp { type | code } | igmp { type } | tcp { src_port_mask < hex 0x0–0xffff > | dst_port_msk <hex 0x0-0xffff> | flag_mask }} | udp { src_port_mask < hex 0x0–0xffff > | dst_port_msk <hex 0x0-0xffff> }] { source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp }]**
Parameter	*profile_id* <*value 1-3*> – Specifies the cpu access profile to be displayed. *ip* - Specifies that the Switch examines the IP fields in each packet with special emphasis on one or more of the following: • *type* – Specifies that the Switch examine each frame's ICMP Type field. • *code* – Specifies that the Switch examine each frame's ICMP code field. • *type* – Specifies that the Switch examine each frame's IGMP Type field. *tcp* – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place. • *src_port_mask* <*hex 0x0-0xffff*> – Specifies the TCP port mask for the source port. • *dst_port_mask* <*hex 0x0-0xffff*> – Specifies the TCP port mask for the destination port. • flag_mask - Specifies the appropriate flag. *udp* – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place. • *src_port_mask* <*0x0-0xffff*> – Specifies the UDP port mask for the source port. • *dst_port_mask* <*0x0-0xffff*> – Specifies the UDP port mask for the destination port mask. • *protocol_id_mask* <*0x0-0xffff*> – Specifies the protocol id mask. • *source_ip_mask* <*netmask*> – Specifies the source IP mask. • *destination_ip_mask* <*netmask*> – Specifies the destination IP mask. • *dscp* – Specifies that the Switch examines the DiffServ Code Point (DSCP) field in each frame's header.

config cpu access_profile (For Ethernet)

The **config cpu access_profile** command configures the settings of cpu access profiles.

config cpu access_profile (For Ethernet)	
Syntax	**config cpu access_profile profile_id <value 1-3> [add | delete] access_id [<value 1-5> | auto_assign] ethernet [{802.1p <vlue 0-7> | destination_mac <macaddr> | ethernet_type <hex 0x5dd-0xffff> | ports <portlist> | source_mac <macaddr> | vlan <vlanid 1-4094>}]**
Parameter	*profile_id* <*value 1-3*> – Specifies the cpu access profile to be configured.

[add | *delete]* – Add or delete the profile id.
access_id [<value 1-5> | *auto_assign]* – Specifies the access id value or use auto assign.
ethernet – Specifies that the Switch examine only the layer 2 part of each packet to determine if it is to be filtered or forwarded based on one or more of the following:

- *802.1p <value 0-7>* – Specifies the 802.1p value. The range is between 0 and 7.
- *destination_mac <macaddrf>* – Specifies the destination MAC address.
- *ethernet_type* – Specifies the Ethernet type mask.
- *<portlist>* – Specifies the port or ports to be configured.
- *source_mac <macaddr>* – Specifies the source MAC address.
- *vlan <vlanid 1-4094>* – Specifies the VLAN id.

config cpu access_profile (For IP)

The **config cpu access_profile** command configures the settings of cpu access profiles.

config cpu access_profile (For IP)	
Syntax	**config cpu access_profile profile_id <value 1-3> [add | delete] access_id [<value 1-5> | auto_assign] IP [{destination_ip <ip_addr> | dscp <value 0-63> | icmp [code <value 0-255>| type <value 0-255>] | igmp type <value 0-255> | ports <portlist> | protocol_id <value 0-255> | source_ip <ip_addr> | tcp[dst_port <value 0-65535> | flag<string> | src_port<value 0-65535>] | udp[dst_port<value 0-65535> | src_port<value 0-65535>]}]**
Parameter	*profile_id <value 1-3>* – Specifies the cpu access profile to be displayed. *[add* | *delete]* – Add or delete the profile id. *access_id [<value 1-5>* | *auto_assign]* – Specifies the access id value or use auto assign. *ip* – Specifies that the Switch examine the IP fields in each packet to determine if it will be either forwarded or filtered based on one or more of the following: • *destination_ip <ip_addr>* – Specifies the destination IP address. • *dscp <value 0-63>* – Specifies the DSCP value. *icmp* – Specifies that the Switch examines the Protocol field in each frame's IP header , and that the value must be 1 (Internet Control Message Protocol- ICMP) for the action to take place. • *code <value 0-255>* –Specifies that the Switch examine each frame's ICMP code field. • *type <value 0-255>* –Specifies that the Switch examine each frame's ICMP Type field. *igmp* – Specifies that the Switch examine each frame's protocol field and it must be 2 (Internet Group Management Protocol-IGMP) for the action to take place. • *igmp_type <value 0-255>* – Specifies the IGMP type. *<portlist>* – Specifies the port or ports to be configured. *protocol_id <value 0-255>* – Specifies the protocol id. *source_ip <ip_addr>* –Specifies that the cpu access profile applies only to packets with this source IP address. T*cp* – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place • *dst_port <value 0-65535>* –Specifies that the cpu access profile

applies only to packets that have this TCP destination port in their header.

- *flag* <*string*> – Specifies the appropriate flag parameter.
- *src_port* <*value 0-65535*> –Specifies that the cpu access profile applies only to packets that have this TCP source port in their header.

udp – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place.

- *dst_port* <*value 0-65535*> – Specifies that the cpu access profile applies only to packets that have this UDP destination port in their header.
- *src_port* <*value 0-65535*> – Specifies that the cpu access profile applies only to packets that have this UDP source port in their header.

delete cpu access_profile

The **delete cpu access_profile** command deletes the settings of cpu access profiles.

delete cpu access_profile	
Syntax	**delete cpu access_profile profile_id <value 1-3>**
Parameter	*profile_id* <*value 1-3*> – Specifies the cpu access profile to be deleted.

show cpu access_profile

The **show cpu access_profile** command displays the settings of cpu access profiles.

show cpu access_profile	
Syntax	**show cpu access_profile {profile_id <value 1-3>}**
Parameter	*profile_id* <*value 1-3*> – Specifies the cpu access profile to be displayed.

35 *TRAFFIC SEGMENTATION Commands*

The Traffic Segmentation commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config traffic_segmentation	<portlist> forward_list [null | <portlist>]
show traffic_segmentation	{<portlist>}

Each command is listed in detail, as follows:

config traffic_segmentation

The **config traffic_segmentation** command configures traffic segmentation on the Switch.

config traffic_segmentation	
Syntax	**config traffic_segmentation <portlist> forward_list [null | <portlist>]**
Parameter	*<portlist>* – A port or a port channel for which the current traffic segmentation configuration on the Switch is to be displayed. *forward_list* – Specifies a port or a port channel to receive forwarded frames from the source ports specified in the portlist, above.

show traffic_segmentation

The **show traffic_segmentation** command displays the current traffic segmentation configuration on the Switch.

show traffic_segmentation	
Syntax	**show traffic_segmentation {<portlist>}**
Parameter	*<portlist>* – A port or a port channel for which the current traffic segmentation configuration on the Switch is to be displayed.

36 *SAFEGUARD Commands*

The Safeguard commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config safeguard_engine	state [enable | disable]
show safeguard_engine	

Each command is listed in detail, as follows:

config safeguard_engin

The **config safeguard_engine state** command is used to enable or disable the safeguard engine on the switch.

config safeguard_engine	
Syntax	**config safeguard_engine state [enable | disable]**
Parameter	None.

show safeguard_engine

The **show safeguard_engine** command is used to show the safeguard engine on the switch.

show safeguard_engine	
Syntax	**show safeguard_engine**
Parameter	None.