D-Link®
Building Networks for People

CLI Reference Guide

Product Model: DWS-3160 Series
Gigabit Ethernet Unified Switch
Release 1.00

Table of Contents

Chapter 1 Using Command Line Interface

The Switch can be managed through the Switch's Command Line Interface (CLI), Web User Interface (Web UI) and by using the Simple Network Management Protocol (SNMP). The Command Line Interface (CLI) can be used to configure and manage the Switch via the serial port or TELNET interfaces.

This manual provides a reference for all of the commands contained in the CLI. Every command will be introduced in terms of purpose, format, description, parameters, and examples. Configuration and management of the Switch via the Web UI is discussed in the Web UI Reference Guide. For detailed information on installing hardware please also refer to the Hardware Installation Guide.

1-1 Accessing the Switch via the Serial Port

The front panel of the Switch provides a port that enables a connection to a computer monitoring and configuring the Switch. The console port is an RJ-45 port and requires a special cable that is included with the Switch, to establish the physical connection.

To use the console port, the following equipment is needed:

1. A terminal or a computer with both an RS-232 serial port and the ability to emulate a terminal.
2. A console cable with a male DB-9 connector on one end and an RJ-45 connection on the other. This cable should be included with the Switch. It establishes the physical connection to the console port.

Using a terminal to connect to the console port:

Connect the male DB-9 connector on the console cable (shipped with the Switch) to the RS-232 serial port on the computer running terminal emulation software then insert the RJ-45 connector into the RJ-45 console port on the front of the Switch.

Set the terminal emulation software as follows:

- Select the appropriate serial port (COM1 or COM2).
- Set the data rate to 115200 baud.
- Set the data format to 8 data bits, 1 stop bit, and no parity.
- Set flow control to none.
- Under Properties, select VT100 for Emulation mode.
- Select Terminal keys for Function, Arrow and Ctrl keys. Make sure to use Terminal keys (not Windows keys) are selected.

NOTE: When using HyperTerminal with the Microsoft® Windows® 2000 operating system, ensure that Windows 2000 Service Pack 2 or later is installed. Windows 2000 Service Pack 2 allows use of arrow keys in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

After correctly configuring the terminal, plug the power cable into the power receptacle on the back of the Switch. The boot sequence will appear in the terminal.

```
  Boot Procedure                                              V1.00.001
-------------------------------------------------------------------------------

  Power On Self Test ........................................  100 %

  MAC Address   : 00-01-02-03-04-00
  H/W Version   : A1

  Please Wait, Loading V1.00.034 Runtime Image ..............  100 %
  UART init ..................................................  100 %
  Starting runtime image
  Device Discovery ...........................................  100 %
  Configuration init .........................................      |
```

After the boot sequence has been completed, the console login screen will be displayed.

The Switch supports user-based security that can allow prevention of unauthorized users from accessing the Switch or changing its settings. This section will explain how to log into the Switch's Command Line Interface via the out-of-band console connection.

Upon initial connection to the Switch, the login screen appears (see example below).

```
                      DWS-3160-24PC Gigabit Ethernet Switch
                             Command Line Interface

                            Firmware: Build 1.00.034
           Copyright(C) 2012 D-Link Corporation. All rights reserved.

UserName:
PassWord:

DWS-3160-24PC:admin#
```

By default, there is no **Username** and **Password** configured in the account settings of this Switch. This will allow the user to simply connect to this Switch for the first time by pressing the '**Enter**' key twice.

After press **Enter** for both the Username and Password fields, access will be given to enter commands after the command prompt (**DWS-3160-24PC:admin#**) appears.

NOTE: The first user automatically gets Administrator level privileges. At least one Admin-level user account must be created for the Switch.

1-2 Setting the Switch's IP Address

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP applications. The Switch's default IP address is 10.90.90.90. You can change the Switch's default IP address to fit into your networking address range.

The Switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found by entering the command "**show switch**" into the command line interface, as displayed below.

```
DWS-3160-24PC:admin#show switch
Command: show switch

Device Type                : DWS-3160-24PC Gigabit Ethernet Switch
MAC Address                : 00-11-22-33-45-67
IP Address                 : 10.90.90.90 (Manual)
VLAN Name                  : default
Subnet Mask                : 255.0.0.0
Default Gateway            : 0.0.0.0
Boot PROM Version          : Build 1.00.001
Firmware Version           : Build 1.00.034
Hardware Version           : A1
System Name                :
System Location            :
System Uptime              : 0 days, 6 hours, 39 minutes, 0 seconds
System Contact             :
Spanning Tree              : Disabled
GVRP                       : Disabled
IGMP Snooping              : Disabled
MLD Snooping               : Disabled
VLAN Trunk                 : Disabled
Telnet                     : Enabled (TCP 23)
Web                        : Enabled (TCP 80)
SNMP                       : Disabled
SSL Status                 : Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

The IP address of the Switch must be configured before it can be managed, by the user, via the Web User Interface.

An example to change the IP address of the Switch to '10.90.90.91', using a subnet mask of '255.0.0.0':

```
DWS-3160-24PC:admin#config ipif System ipaddress 10.90.90.91/8
Command: config ipif System ipaddress 10.90.90.91/8

Success.

DWS-3160-24PC:admin#
```

- At the CLI command prompt, enter the '**config ipif System ipaddress 10.90.90.91/8**' command and press '**Enter'**. This will change the IP address of the Switch to 10.90.90.91.
- Also notice the subnet mask's notation method. Here we use the value '/8' which means that the subnet mask will be change to 255.0.0.0 using the CIDR notation.
- Alternatively, if you don't know the CIDR notation for your subnet mask, you can also simply type out the subnet mask. For example: '**config ipif System ipaddress 10.90.90.91/255.0.0.0**'.

The Switch can now be configured and accessed using TELNET or the Web-based management. The Switch's IP address can also automatically be obtained by using the BOOTP or DHCP protocol.

There are a number of helpful features included in the CLI. Entering the '**?'** command will display a list of all of the top-level commands.

```
DWS-3160-24PC:admin#?
Command: ?

..
?
cable_diag ports
cd
cfm linktrace
cfm lock md
cfm loopback
change drive
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear attack_log
clear cfm pkt_cnt
clear counters
clear ethernet_oam ports
clear fdb
clear igmp_snooping data_driven_group
clear igmp_snooping statistics counter
clear log
clear mac_based_access_control auth_state
clear mld_snooping data_driven_group
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

When entering a command without its required parameters, the CLI will prompt you with a **Next possible completions:** message.

```
DWS-3160-24PC:admin# config account
Command: config account
Next possible completions:
<username>

DWS-3160-24PC:admin#
```

In this case, the command '**config account**' was entered with the parameter **<username>**. The CLI will then prompt to enter the **<username>** with the message, **Next possible completions:**. Every command in the CLI has this feature, and complex commands have several layers of parameter prompting. In addition, after typing any given command plus one space, users can see all of the next possible sub-commands, in sequential order, by repeatedly pressing the **Tab** key.

To re-enter the previous command at the command prompt, press the up arrow cursor key. The previous command will appear at the command prompt.

If a command is entered that is unrecognized by the CLI, the top-level commands will be displayed under the **Available commands:** prompt.

```
DWS-3160-24PC:admin#the
Available commands:
..                  ?                   cable_diag          cd
cfm                 change              clear               config
copy                create              debug               del
delete              dir                 disable             download
enable              erase               format              install
login               logout              md                  move
no                  ping                ping6               rd
reboot              reconfig            rename              reset
save                show                telnet              traceroute
traceroute6         upload

DWS-3160-24PC:admin#
```

The top-level commands consist of commands such as '**show**' or '**config**'. Most of these commands require one or more parameters to narrow the top-level command. This is equivalent to **show** what? or **config** what? Where the what? is the next parameter.

For example, entering the **show** command with no additional parameters, the CLI will then display all of the possible next parameters.

```
DWS-3160-24PC:admin#show
Command: show
Next possible completions:
802.1p              802.1x              access_profile      account
accounting          acct_client         address_binding
arp_spoofing_prevention                 arpentry            asymmetric_vlan
attack_log          auth_client         auth_diagnostics
```

```
auth_session_statistics                 auth_statistics     authen
authen_enable       authen_login        authen_policy       authentication
authorization       autoconfig          bandwidth_control   boot_file
bpdu_protection     captive_portal      cfm                 command
command_history     config              cpu                 current_config
device_status       dhcp_local_relay    dhcp_relay          dlms
dot1v_protocol_group                    dscp
egress_access_profile                   egress_flow_meter   environment
erps                error               ethernet_oam        fdb
filter              flow_meter          gratuitous_arp      greeting_message
gvrp                hol_prevention      igmp_snooping       ipfdb
ipif                ipif_ipv6_link_local_auto               iproute
ipv6                ipv6route           jumbo_frame         lacp_port
limited_multicast_addr                  link_aggregation    lldp
log                 log_save_timing     log_software_module
loopdetect          mac_based_access_control
mac_based_access_control_local          mac_based_vlan      mac_notification
max_mcast_group     mcast_filter_profile                    mirror
mld_snooping        multicast           multicast_fdb       nlb
packet              password_recovery   per_queue           poe
port                port_group          port_security
port_security_entry                     port_vlan           ports
power_saving        private_vlan        pvid                qinq
radius              rmon                router_ports        rspan
safeguard_engine    scheduling          scheduling_mechanism
serial_port         session             sflow               sim
snmp                sntp                ssh                 ssl
storage_media_info                      stp                 switch
syslog              system_severity     tech_support        terminal
time                time_range          traffic
traffic_segmentation                    trap                trusted_host
utilization         vlan                vlan_translation    vlan_trunk
voice_vlan          vrrp                wireless

DWS-3160-24PC:admin#
```

In the above example, all of the possible next parameters for the '**show**' command are displayed.

1-3 Command Syntax Symbols

Syntax	Description
angle brackets < >	Encloses a variable or value. Users must Specifies the variable or value. For example, in the syntax **create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {secondary | state [enable | disable] | proxy_arp [enable | disable] {local [enable | disable]}}** users must supply an IP interface name for **<ipif_name 12>** ,a VLAN name for **<vlan_name 32>** and an address for **<network_address>** when entering the command. DO NOT TYPE THE ANGLE

	BRACKETS.
square brackets [ ]	Encloses a required value or list of required arguments. Only one value or argument must be specified. For example, in the syntax **create account [admin | operator | power_user | user] <username 15> {encrypt [plain_text | sha_1] <password>}** users must Specifies either the admin-level or user-level account when entering the command. DO NOT TYPE THE SQUARE BRACKETS.
vertical bar |	Separates mutually exclusive items in a list, one of which must be entered. For example, in the syntax **create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {secondary | state [enable | disable] | proxy_arp [enable | disable] {local [enable | disable]}}** users must Specifies either the community or trap receiver in the command. DO NOT TYPE THE VERTICAL BAR.
braces { }	Encloses an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax **reset {[config | system]} {force_agree}** users may choose configure or system in the command. DO NOT TYPE THE BRACES.
parentheses ( )	Indicates at least one or more of the values or arguments in the preceding syntax enclosed by braces must be specified. For example, in the syntax **config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown]}(1)** users have the option to Specifies hops or time or both of them. The "(1)" following the set of braces indicates at least one argument or value within the braces must be specified. DO NOT TYPE THE PARENTHESES.
ipif <ipif_name 12> metric <value 1-31>	**12** means the maximum length of the IP interface name. **1-31** means the legal range of the metric value.

1-4 Line Editing Keys

After multiple line command, like ‘**show switch**’, has been entered, the information will be displayed in screen pauses when the command output reaches the end of the page.

```
DWS-3160-24PC:admin#show switch
Command: show switch

Device Type                 : DWS-3160-24PC Gigabit Ethernet Switch
MAC Address                 : 00-11-22-33-45-67
IP Address                  : 10.90.90.90 (Manual)
VLAN Name                   : default
Subnet Mask                 : 255.0.0.0
Default Gateway             : 0.0.0.0
Boot PROM Version           : Build 1.00.001
Firmware Version            : Build 1.00.034
Hardware Version            : A1
System Name                 :
System Location             :
System Uptime               : 0 days, 6 hours, 39 minutes, 0 seconds
System Contact              :
Spanning Tree               : Disabled
GVRP                        : Disabled
IGMP Snooping               : Disabled
MLD Snooping                : Disabled
VLAN Trunk                  : Disabled
Telnet                      : Enabled (TCP 23)
Web                         : Enabled (TCP 80)
SNMP                        : Disabled
SSL Status                  : Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

In the below table, all possible keystroke commands for the screen pause and the normal command prompt are explained.

Keys	Description
CTRL+C	Quit from displaying more pages and return to the command prompt.
ESC	Quit from displaying more pages and return to the command prompt.
q	Quit from displaying more pages and return to the command prompt.
Space or n	Display the next page.
p	Display the previous page.
Enter	Display the next line.
a	Display the remaining pages. (The screen display will not pause again.)
Delete	Delete character under cursor and shift remainder of line to left.
Backspace	Delete character to left of cursor and shift remainder of line to left.
Insert	Toggle on and off. When toggled on, inserts text and shifts previous text to right.
Left Arrow	Move cursor to left.
Right Arrow	Move cursor to right
Tab	Help user to select appropriate token.

R	refresh the displayed pages

Chapter 2 Basic Command List

show session

show serial_port

config serial_port {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}

enable clipaging

disable clipaging

login

logout

? {<Command>}

clear

show command_history

config command_history <value 1-40>

config greeting_message {default}

show greeting_message

config command_prompt [<string 16> | username | default]

config terminal width [default | <value 80-200>]

show terminal width

config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]}] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | mdix [auto | normal | cross] | [description <desc 1-32> | clear_description]}

show ports {<portlist>} {[description | err_disabled | details | media_type]}

2-1 show session

Description

This command is used to display a list of users that are currently accessing the CLI interface.

Format

show session

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display a list of users that is currently accessing the CLI interface:

```
DWS-3160-24PC:admin#show session
Command: show session

 ID  Live Time    From                                    Level User
 --- ------------ --------------------------------------- ----- ---------------
 8   01:35:03.410 Serial Port                             admin Anonymous

Total Entries: 1

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

2-2 show serial_port

Description

This command is used to display the serial port configuration.

Format

show serial_port

Parameters

None.

Restrictions

None.

Example

To display the serial port configuration:

```
DWS-3160-24PC:admin#show serial_port
Command: show serial_port

 Baud Rate     : 115200
 Data Bits     : 8
 Parity Bits   : None
 Stop Bits     : 1
 Auto-Logout   : Never

DWS-3160-24PC:admin#
```

2-3 config serial_port

Description

This command is used to configure the serial port configuration, which includes the bit rate that will be used to communicate with the management host and the automatic logout time for idled connections.

Format

config serial_port {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}

Parameters

baud_rate - (Optional) Specifies the serial bit rate that will be used to communicate with the management host. **9600** - Specifies the serial bit rate to be 9600. **19200** - Specifies the serial bit rate to be 19200. **38400** - Specifies the serial bit rate to be 38400. **115200** - Specifies the serial bit rate to be 115200. This is the default option.
auto_logout - (Optional) Specifies the automatic logout time setting: **never** – Specifies to never timeout. **2_minutes** – Specifies that the automatic logout time will be set to 2 minutes. **5_minutes** - Specifies that the automatic logout time will be set to 5 minutes. **10_minutes** - Specifies that the automatic logout time will be set to 10 minutes. **15_minutes** - Specifies that the automatic logout time will be set to 15 minutes.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure baud rate:

```
DWS-3160-24PC:admin#  config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

Success.

DWS-3160-24PC:admin#
```

2-4 enable clipaging

Description

This command is used to enable the CLI paging command that enables the pausing of the screen display when the output reaches the end of the page. For those show commands that provide the display refresh function, the display will not be refreshed when clipaging is disabled. The default setting is enabled.

Format

enable clipaging

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable pausing of the screen display when show command output reaches the end of the page:

```
DWS-3160-24PC:admin# enable clipaging
Command: enable clipaging

Success.

DWS-3160-24PC:admin#
```

2-5 disable clipaging

Description

This command is used to disable the CLI paging command that disables the pausing of the screen display when the output reaches the end of the page. The default setting is enabled.

Format

disable clipaging

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable pausing of the screen display when the output reaches the end of the page:

```
DWS-3160-24PC:admin#  disable clipaging
Command: disable clipaging

Success.

DWS-3160-24PC:admin#
```

2-6 login

Description

This command is used to allow the user to login to the CLI Interface of the Switch.

Format

login

Parameters

None.

Restrictions

None.

Example

To login the Switch with a username dlink:

```
DWS-3160-24PC:admin# login
Command: login

UserName:dlink
PassWord:****

DWS-3160-24PC:admin#
```

2-7 logout

Description

This command is used to logout from the CLI interface of the Switch.

Format

logout

Parameters

None.

Restrictions

None.

Example

To logout from the CLI Interface of the Switch:

```
DWS-3160-24PC:admin#  logout
Command: logout


**********
* Logout *
**********

                      DWS-3160-24PC Gigabit Ethernet Switch
                              Command Line Interface

                             Firmware: Build 1.00.034
           Copyright(C) 2012 D-Link Corporation. All rights reserved.

UserName:
```

2-8 ?

Description

This command is used to display the usage and description information for a specific command.

Format

? {<Command>}

Parameters

<Command> - (Optional) Enter the CLI command, that the usage and description information is needed from, here.

If no parameter is specified, then all top-level commands will be displayed.

Restrictions

None.

Example

To get “ping” command’s usage and description information:

```
DWS-3160-24PC:admin#? ping
Command: ? ping

Command: ping
Usage:  <ipaddr> { times <value 1-255> | timeout <sec 1-99>}
Description: Used to test the connectivity between network devices.

DWS-3160-24PC:admin#
```

2-9 clear

Description

This command is used to clear the screen.

Format

clear

Parameters

None.

Restrictions

None.

Example

To clear the screen:

```
DWS-3160-24PC:admin# clear
Command: clear



DWS-3160-24PC:admin#
```

2-10 show command_history

Description

The command is used to display command history.

Format

show command_history

Parameters

None.

Restrictions

None.

Example

To display command history:

```
DWS-3160-24PC:admin#show command_history
Command: show command_history

? ping
login
show serial_port
show session
? config bpdu_protection ports
? reset
? create account
? create ipif
show
the
?

DWS-3160-24PC:admin#
```

2-11 config command_history

Description

This command is used to configure the number of commands that the Switch can recall.

Format

config command_history <value 1-40>

Parameters

command_history – Specifies the number of commands that the Switch can recall.
<value 1-40> - Enter the command history value here. This value must be between 1 and 40.

Restrictions

None.

Example

To configure the number of the command history:

```
DWS-3160-24PC:admin# config command_history 25
Command: config command_history 25

Success.

DWS-3160-24PC:admin#
```

2-12 config greeting_message

Description

This command is used to configure the greeting message (or banner).

Format

config greeting_message {default}

Parameters

default - (Optional) Specifies that the greeting message (banner) will be returned to its original factory default state.

Restrictions

Only Administrators and Operators can issue this command.

Example

To edit the banner:

```
DWS-3160-24PC:admin#config greeting_message
Command: config greeting_message

Greeting Messages Editor
==============================================================================

                      DWS-3160-24PC Gigabit Ethernet Switch
                             Command Line Interface

                            Firmware: Build 1.00.034
           Copyright(C) 2012 D-Link Corporation. All rights reserved.
==============================================================================

   <Function Key>                    <Control Key>
   Ctrl+C     Quit without save      left/right/
   Ctrl+W     Save and quit            up/down     Move cursor
                                     Ctrl+D        Delete line
                                     Ctrl+X        Erase all setting
                                     Ctrl+L        Reload original setting
------------------------------------------------------------------------------
```

2-13 show greeting_message

Description

The command is used to display the greeting message.

Format

show greeting_message

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display the greeting message:

```
DWS-3160-24PC:admin#show greeting_message
Command: show greeting_message

==============================================================================

                      DWS-3160-24PC Gigabit Ethernet Switch
                             Command Line Interface

                            Firmware: Build 1.00.034
           Copyright(C) 2012 D-Link Corporation. All rights reserved.

==============================================================================

DWS-3160-24PC:admin#
```

2-14 config command_prompt

Description

This command is used to modify the command prompt in the CLI interface. It will modify the first part with a string consisting of a maximum of 16 characters, or to be replaced with the users' login user name. When users issue the 'reset' command, the current command prompt will remain intact. Yet, issuing the 'reset system' will return the command prompt to its original factory default value.

Format

config command_prompt [<string 16> | username | default]

Parameters

<string 16> - Enter the new command prompt string of no more than 16 characters.
username - Specifies to configure the login username as the command prompt.
default – Specifies to return the command prompt to its original factory default value.

Restrictions

Only Administrators and Operators can issue this command.

Example

To edit the command prompt:

```
DWS-3160-24PC:admin#config command_prompt Prompt#
Command: config command_prompt Prompt#

Success.

Prompt#:admin#
```

2-15 config terminal width

Description

The command is used to set current terminal width.

The usage is described as below:

1. Users login and configure the terminal width to 120, this configuration take effect on this login section. If users implement “save” command, the configuration is saved. After users log out and log in again, the terminal width is 120.
2. If user did not save the configuration, another user login, the terminal width is default value.
3. If at the same time, two CLI sessions are running, once section configure to 120 width and save it, the other section will not be effected, unless it log out and then log in.

Format

config terminal width [default | <value 80-200>]

Parameters

default - The default setting of terminal width. The default value is 80.

<value 80-200> - The terminal width which will be configured. The width is between 80 and 200 characters.

Restrictions

None.

Example

To configure the current terminal width:

```
DWS-3160-24PC:admin# config terminal width 120
Command: config terminal width 120

Success.

DWS-3160-24PC:admin#
```

2-16 show terminal width

Description

The command is used to display the configuration of current terminal width.

Format

show terminal width

Parameters

None.

Restrictions

None.

Example

To display the configuration of current terminal width:

```
DWS-3160-24PC:admin#show terminal width
Command: show terminal width

Global terminal width     : 80
Current terminal width    : 80

DWS-3160-24PC:admin#
```

2-17 config ports

Description

This command is used to configure the Switch's port settings.

Format

config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]}] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | mdix [auto | normal | cross] | [description <desc 1-32> | clear_description]}

Parameters

ports - Specifies a range of ports to be configured. **<portlist>** - Enter a list of ports used here. **all** - Specifies that all the ports will be used for this configuration.
medium_type - (Optional) Specifies the medium type while the configure ports are combo ports **fiber** - Specifies that the medium type will be set to fiber. **copper** - Specifies that the medium type will be set to copper.
speed - (Optional) Specifies the port speed of the specified ports . **auto** - Set port speed to auto negotiation.

10_half - Set port speed to 10_half.
10_full - Set port speed to 10_full.
100_half - Set port speed to 100_half.
100_full - Set port speed to 100_full._
1000_full - 1000_full set port speed to 1000_full. While set port speed to 1000_full,user should Specifies master or slave mode for 1000 base TX interface, and leave the 1000_full without any master or slave setting for other interface.
master - Specifies that the port(s) will be set to master.
slave - Specifies that the port(s) will be set to slave.

flow_control - (Optional) You can turn on or turn off flow control on one or more ports. By set flow_control to enable or disable.
enable - Specifies that the flow control option will be enabled.
disable - Specifies that the flow control option will be disabled.

learning - (Optional) You can turn on or turn off MAC address learning on one or more ports.
enable - Specifies that the learning option will be enabled.
disable - Specifies that the learning option will be disabled.

state - (Optional) Enables or disables the specified port. If the specified ports are in error-disabled status , configure their state to enable will recover these ports from disabled to enable state.
enable - Specifies that the port state will be enabled.
disable - Specifies that the port state will be disabled.

mdix - (Optional) MDIX mode can be specified as auto, normal, and cross. If set to normal state, the port is in MDIX mode and can be connected to PC NIC using a straight cable. If set to cross state, the port is in mdi mode, and can be connected to a port (in mdix mode) on another Switch thru a straight cable.
auto - Specifies that the MDIX mode for the port will be set to auto.
normal - Specifies that the MDIX mode for the port will be set to normal.
cross - Specifies that the MDIX mode for the port will be set to cross.

description - (Optional) Specifies the description of the port interface.
<desc 1-32> - Enter the port interface description here. This value can be up to 32 characters long.
clear_description - Specifies that the description field will be cleared.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the ports:

```
DWS-3160-24PC:admin#config ports all medium_type copper speed auto
Command: config ports all medium_type copper speed auto

Success.

DWS-3160-24PC:admin#
```

2-18 show ports

Description

This command is used to display the current configurations of a range of ports.

Format

show ports {<portlist>} {[description | err_disabled | details | media_type]}

Parameters

ports - Specifies a range of ports to be displayed.
<portlist> - (Optional) Enter the list of ports to be configured here.

description - (Optional) Indicates if port description will be included in the display .
err_disabled - (Optional) Indicates if ports are disabled by some reasons will be displayed.
details - (Optional) Displays the port details.
media_type - (Optional) Displays port transceiver type.

Restrictions

None.

Example

To display the port details:

```
DWS-3160-24PC:admin#show ports details
Command: show ports details

Port : 1
--------------------
Port Status                 : Link Down
Description                 :
HardWare Type               : Gigabits Ethernet
MAC Address                 : 00-11-22-33-45-77
Bandwidth                   : 1000000Kbit
Auto-Negotiation            : Enabled
Duplex Mode                 : Full Duplex
Flow Control                : Disabled
MDI                         : Auto
Address Learning            : Enabled
Last Clear of Counter       : 0 hours 5 mins ago
BPDU Hardware Filtering Mode: Disabled
Queuing Strategy            : FIFO
TX Load                     :   0/100,      0 bits/sec,        0 packets/sec
RX Load                     :   0/100,      0 bits/sec,        0 packets/sec

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Chapter 3 802.1Q VLAN Command List

create vlan <vlan_name 32> tag <vlanid 2-4094> {type [1q_vlan | private_vlan]} {advertisement}
create vlan vlanid <vidlist> {type [1q_vlan | private_vlan]} {advertisement}
delete vlan <vlan_name 32>
delete vlan vlanid <vidlist>
config vlan <vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}(1)
config vlan vlanid <vidlist> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable] | name <vlan_name 32>}(1)
config port_vlan [<portlist> | all] {gvrp_state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}(1)
show vlan {<vlan_name 32>}
show vlan ports {<portlist>}
show vlan vlanid <vidlist>
show port_vlan {<portlist>}
enable pvid auto_assign
disable pvid auto_assign
show pvid auto_assign
config gvrp [timer {join <value 100-100000> | leave <value 100-100000> | leaveall <value 100-100000> } | nni_bpdu_addr [dot1d | dot1ad]]
show gvrp
enable gvrp
disable gvrp
config private_vlan [<vlan_name 32> | vid <vlanid 1-4094>] [add [isolated | community] | remove] [<vlan_name 32> | vlanid <vidlist>]
show private_vlan {[<vlan_name 32> | vlanid<vidlist>]}

3-1 create vlan

Description

The command is used to create a VLAN on the Switch. The VLAN ID must always be specified when creating a VLAN.

Format

create vlan <vlan_name 32> tag <vlanid 2-4094> {type [1q_vlan | private_vlan]} {advertisement}

Parameters

vlan - The name of the VLAN to be created. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
tag - The VLAN ID of the VLAN to be created. **<vlanid 2-4094>** - Enter the VLAN ID here. The VLAN ID value must be between 2 and 4094.
type - (Optional) Specifies the type of VLAN here. **1q_vlan** - (Optional) Specifies that the type of VLAN used is based on the 802.1Q standard. **private_vlan –** (Optional) Specifies that the private VLAN type will be used.
advertisement - (Optional) Specifies the VLAN as being able to be advertised out.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a VLAN with name “v2” and VLAN ID 2:

```
DWS-3160-24PC:admin# create vlan v2 tag 2 type 1q_vlan advertisement
Command: create vlan v2 tag 2 type 1q_vlan advertisement

Success.

DWS-3160-24PC:admin#
```

3-2 create vlan vlanid

Description

The command is used to create more than one VLAN at a time. A unique VLAN name will be automatically assigned by the system.

The automatic assignment of the VLAN name is based on the following rule:

1. ‘VLAN’+ID. For example, if the VLAN ID is 100, the VLAN name will be ‘VLAN100’. If this VLAN name is in conflict with the name of an existing VLAN, then it will be renamed based on the following rule:
2. ‘VLAN’+ID+’ALT’+collision count. For example, if this conflict is the second collision, then the name will be ‘VLAN100ALT2’.

Format

create vlan vlanid <vidlist> {type [1q_vlan | private_vlan]} {advertisement}

Parameters

vlanid - The VLAN ID list to be created.
  <vidlist> - Enter the VLAN ID list here.

type - (Optional) Specifies the type of VLAN to be created.
  1q_vlan - (Optional) Specifies that the VLAN created will be a 1Q VLAN.
  private_vlan – (Optional) Specifies that the private VLAN type will be used.

advertisement - (Optional) Specifies the VLAN as being able to be advertised out.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a couple of VLANs using VLAN ID method:

```
DWS-3160-24PC:admin# create vlan vlanid 10-30
Command: create vlan vlanid 10-30

Success.

DWS-3160-24PC:admin#
```

3-3 delete vlan

Description

This command is used to delete a previously configured VLAN by the name on the Switch.

Format

delete vlan <vlan_name 32>

Parameters

vlan - The VLAN name of the VLAN to be deleted.
<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To remove a vlan v1:

```
DWS-3160-24PC:admin# delete vlan v1
Command: delete vlan v1

Success.

DWS-3160-24PC:admin#
```

3-4 delete vlan vlanid

Description

This command is used to delete one or a number of previously configured VLANs by using the VLAN ID list.

Format

delete vlan vlanid <vidlist>

Parameters

vlanid - The VLAN ID list to be deleted.
<vidlist> - Enter the VLAN ID list here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To remove VLANs from 10-30:

```
DWS-3160-24PC:admin# delete vlan vlanid 10-30
Command: delete vlan vlanid 10-30

Success.

DWS-3160-24PC:admin#
```

3-5 config vlan

Description

This command is used to configure a VLAN based on the name.

Format

config vlan <vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}(1)

Parameters

vlan - The name of the VLAN you want to add ports to.
<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

add - (Optional) Specifies to add tagged, untagged or forbidden ports to the VLAN.
tagged - Specifies the additional ports as tagged.
untagged - Specifies the additional ports as untagged.
forbidden - Specifies the additional ports as forbidden.

delete - (Optional) Specifies to delete ports from the VLAN.

<portlist> - (Optional) Enter the list of ports used for the configuration here.

advertisement - (Optional) Specifies the GVRP state of this VLAN.
enable - Specifies to enable advertisement for this VLAN.
disable - Specifies to disable advertisement for this VLAN.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add ports, 4 to 8, to the VLAN called ‘v1’, as tagged ports:

```
DWS-3160-24PC:admin# config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DWS-3160-24PC:admin#
```

3-6 config vlan vlanid

Description

The command is used to configure multiple VLANs at the same time. Conflicts might be generated if you configure the name of multiple VLANs at the same time.

Format

config vlan vlanid <vidlist> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable] | name <vlan_name 32>}(1)

Parameters

vlanid - The VID list of VLANs to configure.
  <vidlist> - Enter the VLAN ID list here.

add - (Optional) Specifies to add tagged, untagged or forbidden ports to the VLAN.
  tagged - Specifies the additional ports as tagged.
  untagged - Specifies the additional ports as untagged.
  forbidden - Specifies the additional ports as forbidden.

delete - (Optional) Specifies to delete ports from the VLAN.

<portlist> - (Optional) Enter the list of ports used for the configuration here.

advertisement - (Optional) Specifies the GVRP state of this VLAN.
  enable - Specifies to enable advertisement for this VLAN.
  disable - Specifies to disable advertisement for this VLAN.

name - (Optional) The new name of the VLAN.
  <vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add ports, 4 to 8, to VLANs ranging from VLAN ID 10 to VLAN ID 20, as tagged ports:

```
DWS-3160-24PC:admin# config vlan vlanid 10-20 add tagged 4-8
Command: config vlan vlanid 10-20 add tagged 4-8

Success.

DWS-3160-24PC:admin#
```

3-7 config port_vlan

Description

This command is used to configure the ingress checking status of sending and receiving GVRP information.

Format

config port_vlan [<portlist> | all] {gvrp_state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}(1)

Parameters

port_vlan - Specifies that the following will be applied to the port VLAN. **<portlist>** - A range of ports for which you want ingress checking. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then highest Switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. **all** - Specifies that all the port will be used for this configuration.
gvrp_state - (Optional) Enabled or disables GVRP for the ports specified in the port list. **enable** - Specifies that GVRP for the specified ports will be enabled. **disable** - Specifies that GVRP for the specified ports will be disabled.
ingress_checking - (Optional) Enables or disables ingress checking for the specified portlist. **enable** - Specifies that ingress checking will be enabled for the specified portlist. **disable** - Specifies that ingress checking will be disabled for the specified portlist.
acceptable_frame - (Optional) The type of frame will be accepted by the port. There are two types: **tagged_only** - Only tagged packets can be accepted by this port. **admit_all** - All packets can be accepted.
pvid - (Optional) Specifies the PVID of the ports. **<vlanid 1-4094>** - Enter the VLAN ID here. The VLAN ID value must be between 1 and 4094.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the ingress checking status of sending and receiving GVRP information:

```
DWS-3160-24PC:admin# config gvrp 1-5 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2
Command: config gvrp 1-5 state enable ingress_checking enable acceptable_frame
tagged_only pvid 2

Success

DWS-3160-24PC:admin# config port_vlan 1-5 gvrp_state enable ingress_checking
enable acceptable_frame tagged_only pvid 2
Command: config port_vlan 1-5 gvrp_state enable ingress_checking enable
acceptable_frame tagged_only pvid 2

Success

DWS-3160-24PC:admin#
```

3-8 show vlan

Description

This command is used to display VLAN information, including parameters settings and operational values.

Format

show vlan {<vlan_name 32>}

Parameters

vlan - Specifies the VLAN to be displayed.

<vlan_name 32> - (Optional) Enter the VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

None.

Example

To display the VLAN settings:

```
DWS-3160-24PC:admin#show vlan
Command: show vlan

VLAN Trunk State        : Disabled
VLAN Trunk Member Ports :

VID             : 1               VLAN Name     : default
VLAN Type       : Static          Advertisement : Enabled
Member Ports    : 1-24
Static Ports    : 1-24
Current Tagged Ports  :
Current Untagged Ports: 1-24
Static Tagged Ports   :
Static Untagged Ports : 1-24
Forbidden Ports       :

Total Static VLAN Entries: 1
Total GVRP VLAN Entries: 0

DWS-3160-24PC:admin#
```

3-9 show vlan ports

Description

This command is used to display the VLAN configuration per port.

Format

show vlan ports {<portlist>}

Parameters

port - (Optional) Specifies the list of ports for which the VLAN information will be displayed.
<portlist> - Enter the list of ports that will be displayed here.

Restrictions

None.

Example

To display the VLAN configuration for port 6:

```
DWS-3160-24PC:admin#show vlan ports 6
Command: show vlan ports 6

 Port   VID   Untagged  Tagged  Dynamic  Forbidden
-----   ----  --------  ------  -------  ---------
 6      1       X         -       -        -

DWS-3160-24PC:admin#
```

3-10 show vlan vlanid

Description

This command is used to display VLAN information using the VLAN ID.

Format

show vlan vlanid <vidlist>

Parameters

vlanid - (Optional) Specifies the VLAN ID of the VLAN.
<vidlist> - Enter the VLAN ID here.

Restrictions

None.

Example

To display the VLAN configuration for VLAN ID 1:

```
DWS-3160-24PC:admin#show vlan vlanid 1
Command: show vlan vlanid 1

VID             : 1              VLAN Name     : default
VLAN Type       : Static         Advertisement : Enabled
Member Ports    : 1-24
Static Ports    : 1-24
Current Tagged Ports  :
Current Untagged Ports: 1-24
Static Tagged Ports   :
Static Untagged Ports : 1-24
Forbidden Ports       :

 Total Entries : 1

DWS-3160-24PC:admin#
```

3-11 show port_vlan

Description

This command is used to display the ports' VLAN attributes on the Switch.

Format

show port_vlan {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be displayed.
If no parameter specified, system will display all ports gvrp information.

Restrictions

None.

Example

To display the 802.1Q port setting:

```
DWS-3160-24PC:admin#show port_vlan
Command: show port_vlan

Port     PVID  GVRP      Ingress Checking  Acceptable Frame Type
-------  ----  --------  ----------------  ---------------------------
 1       1     Disabled  Enabled           All Frames
 2       1     Disabled  Enabled           All Frames
 3       1     Disabled  Enabled           All Frames
 4       1     Disabled  Enabled           All Frames
 5       1     Disabled  Enabled           All Frames
 6       1     Disabled  Enabled           All Frames
 7       1     Disabled  Enabled           All Frames
 8       1     Disabled  Enabled           All Frames
 9       1     Disabled  Enabled           All Frames
 10      1     Disabled  Enabled           All Frames
 11      1     Disabled  Enabled           All Frames
 12      1     Disabled  Enabled           All Frames
 13      1     Disabled  Enabled           All Frames
 14      1     Disabled  Enabled           All Frames
 15      1     Disabled  Enabled           All Frames
 16      1     Disabled  Enabled           All Frames
 17      1     Disabled  Enabled           All Frames
 18      1     Disabled  Enabled           All Frames
 19      1     Disabled  Enabled           All Frames
 20      1     Disabled  Enabled           All Frames
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3-12 enable pvid auto assign

Description

The command is used to enable the auto-assignment of PVID.

If this feature is enabled, the PVID will possibly be changed by the PVID or the VLAN configuration. When a user configures a port to VLAN X’s untagged membership, this port’s PVID will be updated with VLAN X. The PVID is updated with the last item of the VLAN list. When a user removes a port from the untagged membership of the PVID’s VLAN, the port’s PVID will be assigned with a ‘default VLAN’ parameter.

By default, this setting is enabled.

Format

enable pvid auto_assign

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the auto-assign PVID:

```
DWS-3160-24PC:admin# enable pvid auto_assign
Command: enable pvid auto_assign

Success.

DWS-3160-24PC:admin#
```

3-13 disable pvid auto assign

Description

This command is used to disable auto-assignment of the PVID.

Format

disable pvid auto_assign

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the auto-assign PVID:

```
DWS-3160-24PC:admin# disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DWS-3160-24PC:admin#
```

3-14 show pvid auto_assign

Description

This command is used to display the PVID auto-assignment state.

Format

show pvid auto_assign

Parameters

None.

Restrictions

None.

Example

To display PVID auto-assignment state:

```
DWS-3160-24PC:admin#show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled

DWS-3160-24PC:admin#
```

3-15 config gvrp

Description

The command is used to configure the Generic VLAN Registration Protocol (GVRP) timer value.

Format

config gvrp [timer {join <value 100-100000> | leave <value 100-100000> | leaveall <value 100-100000> } | nni_bpdu_addr [dot1d | dot1ad]]

Parameters

timer - Specifies that the GVRP timer parameter will be configured.
join - (Optional) Specifies the Join time will be set. **<value 100-100000>** - Enter the join time used here. This value must be between 100 and 100000. The default value is 200 milliseconds.
leave - (Optional) Specifies the Leave time will be set. **<value 100-100000>** - Enter the leave time used here. This value must be between 100 and 100000. The default value is 600 milliseconds.
leaveall - (Optional) Specifies the LeaveAll time will be set. **<value 100-100000>** - Enter the leave all time used here. This value must be between 100 and 100000. The default value is 10000 milliseconds.
nni_bpdu_addr - Used to determine the BPDU protocol address for GVRP in service provide

	site. It can use 802.1d GVRP address, 802.1ad service provider GVRP address or a user defined multicast address. The range of the user defined address is 0180C2000000 - 0180C2FFFFFF. **dot1d** - Specifies that the NNI BPDU protocol address value will be set to Dot1d. **dot1ad** - Specifies that the NNI BPDU protocol address value will be set to Dot1ad.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the Join time to 200 milliseconds:

```
DWS-3160-24PC:admin# config gvrp timer join 200
Command: config gvrp timer join 200

Success.

DWS-3160-24PC:admin#
```

3-16 show gvrp

Description

This command is used to display the GVRP global setting.

Format

show gvrp

Parameters

None.

Restrictions

None.

Example

To display the global setting of GVRP:

```
DWS-3160-24PC:admin#show gvrp
Command: show gvrp

 Global GVRP   : Disabled
 Join Time     : 200 Milliseconds
 Leave Time    : 600 Milliseconds
 LeaveAll Time : 10000 Milliseconds
 NNI BPDU Address: dot1d

DWS-3160-24PC:admin#
```

3-17 enable gvrp

Description

This command is used to enable GVRP.

Format

enable gvrp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable GVRP:

```
DWS-3160-24PC:admin# enable gvrp
Command: enable gvrp

Success.

DWS-3160-24PC:admin#
```

3-18 disable gvrp

Description

This command is used to disable GVRP.

Format

disable gvrp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable GVRP:

```
DWS-3160-24PC:admin# disable gvrp
Command: disable gvrp

Success.

DWS-3160-24PC:admin#
```

3-19 config private_vlan

Description

This command is used to add or remove a secondary VLAN from a private VLAN.

Format

config private_vlan [<vlan_name 32> | vid <vlanid 1-4094>] [add [isolated | community] | remove] [<vlan_name 32> | vlanid <vidlist>]

Parameters

<vlan_name 32> - Specifies the name of the private VLAN.
  vid - Specifies the VLAN ID of the private VLAN
    <vlanid 1-4094> - Enter the VLAN ID used here. This value must be between 1 and 4094.

add - Specifies that a secondary VLAN will be added to the private VLAN.
  isolated - Specifies the secondary VLAN as isolated VLAN.
  community - Specifies the secondary VLAN as community VLAN
remove - Specifies that a secondary VLAN will be removed from the private VLAN.

<vlan_name 32> - Specifies the secondary VLAN name used. This name can be up to 32 characters long.
  vlanid - A range of secondary VLAN to add or remove to the private VLAN.
    <vidlist> - Enter the secondary VLAN ID used here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add a secondary VLAN to the private VLAN called ‘p1’:

```
DWS-3160-24PC:admin# config private_vlan p1 add community vlanid 2-5
Command: config private_vlan p1 add community vlanid 2-5

Success.

DWS-3160-24PC:admin#
```

3-20 show private vlan

Description

This command is used to display the private VLAN configuration.

Format

show private_vlan {[<vlan_name 32> | vlanid<vidlist>]}

Parameters

<vlan_name 32> - (Optional) Specifies the name of the private VLAN or its secondary VLAN.
This name can be up to 32 characters long.
vlanid - (Optional) Specifies the VLAN ID of the private VLAN or its secondary VLAN.
<vidlist> - Enter the VLAN ID used here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display the private VLAN configuration:

```
DWS-3160-24PC:admin# show private_vlan
Command: show private_vlan

Private VLAN 100
------------------
    Promiscuous Ports: 1
    Trunk Ports      : 2
    Isolated Ports   : 3-5       Isolated VLAN : 20
    Community Ports  : 6–8       Community VLAN: 30
    Community Ports: : 9–10      Community VLAN: 40

Private VLAN 200
------------------
    Promiscuous Ports: 11
    Trunk Ports      : 12
    Isolated Ports   : 13-15         Isolated VLAN : 20
    Community Ports  : 16–18         Community VLAN: 30

DWS-3160-24PC:admin#
```

Chapter 4 802.1X Command List

enable 802.1x

disable 802.1x

create 802.1x user <username 15>

delete 802.1x user <username 15>

show 802.1x user

config 802.1x auth_protocol [local | radius_eap]

config 802.1x fwd_pdu system [enable | disable]

config 802.1x fwd_pdu ports [<portlist> | all] [enable | disable]

config 802.1x authorization attributes radius [enable | disable]

show 802.1x {[auth_state | auth_configuration] ports {<portlist>}}

config 802.1x capability ports [<portlist> | all] [authenticator | none]

config 802.1x max_users [<value 1–448> | no_limit]

config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both | in] | 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 1-65535> | max_users [<value 1-448> | no_limit] | enable_reauth [enable | disable]}(1)]

config 802.1x auth_mode [port_based | mac_based]

config 802.1x init [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]

config 802.1x reauth [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]

create 802.1x guest_vlan {<vlan_name 32>}

delete 802.1x guest_vlan {<vlan_name 32>}

config 802.1x guest_vlan ports [<portlist> | all] state [enable | disable]

show 802.1x guest_vlan

config radius add <server_index 1-3> [<server_ip> | <ipv6addr>] key <password 32> [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <sec 1-255> | retransmit <int 1-20>}]

config radius delete <server_index 1-3>

config radius <server_index 1-3> {ipaddress [<server_ip> | <ipv6addr>] | key <password 32> | auth_port [<udp_port_number 1-65535> | default] | acct_port [<udp_port_number 1-65535> | default] | timeout [<sec 1-255> | default] | retransmit [<int 1-20> | default]}

show radius

show auth_statistics {ports <portlist>}

show auth_diagnostics {ports <portlist>}

show auth_session_statistics {ports <portlist>}

show auth_client

show acct_client

config accounting service [network | shell | system] state [enable | disable]

show accounting service

4-1 enable 802.1x

Description

This command is used to enable the 802.1X function.

Format

enable 802.1x

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the 802.1X function:

```
DWS-3160-24PC:admin# enable 802.1x
Command: enable 802.1x

Success.

DWS-3160-24PC:admin#
```

4-2 disable 802.1x

Description

This command is used to disable the 802.1X function.

Format

disable 802.1x

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the 802.1X function:

```
DWS-3160-24PC:admin# disable 802.1x
Command: disable 802.1x

Success.

DWS-3160-24PC:admin#
```

4-3 create 802.1x user

Description

This command is used to create an 802.1X user.

Format

create 802.1x user <username 15>

Parameters

user - Specifies adding user name.

<username 15> - Enter the username here. This value can be up to 15 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an 802.1x user called ‘test’:

```
DWS-3160-24PC:admin# create 802.1x user test
Command: create 802.1x user test

Enter a case-sensitive new password:
Enter the new password again for confirmation:

Success.

DWS-3160-24PC:admin#
```

4-4 delete 802.1x user

Description

This command is used to delete an 802.1X user.

Format

delete 802.1x user <username 15>

Parameters

user - Specifies the adding user name.

<username 15> - Enter the username here. This value can be up to 15 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the 802.1X user called ‘test’:

```
DWS-3160-24PC:admin# delete 802.1x user test
Command: delete 802.1x user test

Success.

DWS-3160-24PC:admin#
```

4-5 show 802.1x user

Description

This command is used to display the 802.1X user’s login information.

Format

show 802.1x user

Parameters

None.

Restrictions

None.

Example

To display the 802.1X user’s login information:

```
DWS-3160-24PC:admin# show 802.1x user
Command: show 802.1x user

Username     Password
-----------  ----------
 user1       abcds

Total Entries : 1

DWS-3160-24PC:admin#
```

4-6 config 802.1x auth_protocol

Description

This command is used to configure the 802.1X authentication protocol.

Format

config 802.1x auth_protocol [local | radius_eap]

Parameters

local - Specifies the authentication protocol as local.

radius_eap - Specifies the authentication protocol as RADIUS EAP.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the 802.1X authentication protocol as RADIUS EAP:

```
DWS-3160-24PC:admin# config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.

DWS-3160-24PC:admin#
```

4-7 config 802.1x fwd_pdu system

Description

This command is used to configure the control of forwarding EAPOL PDUs. When the 802.1X functionality is disabled, for a port, and if the 802.1X forwarding PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded on the same VLAN to those ports of which the 802.1X forwarding PDU is enabled and 802.1X is disabled (globally or just for the port).

Format

config 802.1x fwd_pdu system [enable | disable]

Parameters

enable - Enable the forwarding of EAPOL PDU.

disable - Disable the forwarding of EAPOL PDU. This is the default option.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable forwarding of the EAPOL PDU system:

```
DWS-3160-24PC:admin# config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable

Success.

DWS-3160-24PC:admin#
```

4-8 config 802.1x fwd_pdu ports

Description

This command is used to configure the per port setting to control the forwarding of EAPOL PDU. When the 802.1X functionality is disabled globally or for a port, and if the 802.1X forwarding PDU is enabled, both globally and for the port, a received EAPOL packet on the port will be flooded on the same VLAN to those ports for which the 802.1X forwarding PDU option is enabled and 802.1X is disabled (globally or just for the port).

Format

config 802.1x fwd_pdu ports [<portlist> | all] [enable | disable]

Parameters

ports - Specifies a range of ports to be configured. **<portlist>** - Enter the list of ports used for the configuration here. **all** - Specifies that all the ports will be used.
enable - Enable forwarding EAPOL PDU receive on the ports. **disable** - Disable forwarding EAPOL PDU receive on the ports. This is the default option.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the 802.1X forwarding PDU for ports 1 and 2:

```
DWS-3160-24PC:admin# config 802.1x fwd_pdu ports 1,2 enable
Command: config 802.1x fwd_pdu ports 1,2 enable

Success.

DWS-3160-24PC:admin#
```

4-9 config 802.1x authorization attributes

Description

This command is used to enable or disable the 802.1X authorization attributes. When authorization is enabled for 802.1X RADIUS authentication, the authorized attributes assigned by the RADUIS server will be accepted if the global authorization status is enabled.

Format

config 802.1x authorization attributes radius [enable | disable]

Parameters

radius - If specified to enable, the authorization attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted if the global authorization status is enabled. The default state is enabled.
enable - Specifies to enable the authorization attributes.
disable - Specifies to disable the authorization attributes.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the option to accept the authorized data assigned from the RADIUS server:

```
DWS-3160-24PC:admin# config 802.1x authorization attributes radius disable
Command: config 802.1x authorization attributes radius disable

Success.

DWS-3160-24PC:admin#
```

4-10 show 802.1x

Description

This command is used to display the 802.1X state or configurations.

Format

show 802.1x {[auth_state | auth_configuration] ports {<portlist>}}

Parameters

auth_state - (Optional) Used to display 802.1X authentication state machine of some or all ports
auth_configuration - (Optional) Used to display 802.1X configurations of some or all ports.

port - (Optional) Specifies a range of ports to be displayed. If no port is specified, all ports will be displayed.
<portlist> - Enter the list of ports used for the configuration here.

If no parameter is specified, the 802.1X system configurations will be displayed.

Restrictions

None.

Example

To display the 802.1X port level configurations:

```
DWS-3160-24PC:admin# show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

Port Number    : 1
Capability     : None
AdminCrlDir    : Both
OpenCrlDir     : Both
Port Control   : Auto
QuietPeriod    : 60    sec
TxPeriod       : 30    sec
SuppTimeout    : 30    sec
ServerTimeout  : 30    sec
MaxReq         : 2     times
ReAuthPeriod   : 3600  sec
ReAuthenticate : Disabled
Forward EAPOL PDU On Port : Disabled
Max User On Port : 16

DWS-3160-24PC:admin#
```

4-11 config 802.1x capability

Description

This command is used to configure port capabilities.

Format

config 802.1x capability ports [<portlist> | all] [authenticator | none]

Parameters

ports - Specifies a range of ports to be configured.

<portlist> - Enter the list of ports used for the configuration here.

all - Specifies all ports to be configured.

authenticator - The port that wishes to enforce authentication before allowing access to services that are accessible via that port adopts the authenticator role.

none - Disable authentication on the specified ports.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure port capabilities:

```
DWS-3160-24PC:admin# config 802.1x capability ports 1-10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

Success.

DWS-3160-24PC:admin#
```

4-12 config 802.1x max_users

Description

This command is used to configure the maximum number of users that can be learned via 802.1X authentication. In addition to the global limitation, maximum users per port are also limited. It can be configured using the ‘config 802.1x auth_parameter’ command.

Format

config 802.1x max_users [<value 1–448> | no_limit]

Parameters

max_users - Specifies the maximum number of users.

<value 1-448> - Enter the maximum users value here. This value must be between 1 and 448.

no_limit – Specifies that the maximum user limit will be set to 448.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a maximum of 200, 802.1X users:

```
DWS-3160-24PC:admin# config 802.1x max_users 200
Command: config 802.1x max_users 200

Success.

DWS-3160-24PC:admin#
```

4-13 config 802.1x auth_parameter

Description

This command is used to configure the parameters that control the operation of the authenticator associated with a port.

Format

config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both | in] | 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 1-65535> | max_users [<value 1-448> | no_limit] | enable_reauth [enable | disable]}(1)]

Parameters

ports - Specifies a range of ports to be configured.
<portlist> - Enter the list of ports used for the configuration here.
all - Specifies that all the ports will be used.

default - Sets all parameter to be default value.

direction - (Optional) Sets the direction of access control.
both - For bidirectional access control.
in - For unidirectional access control.

port_control - (Optional) You can force a specific port to be unconditionally authorized or unauthorized by setting the parameter of port_control to be force authorized or force unauthorized. Besides, the controlled port will reflect the outcome of authentication if port_control is auto.
force_unauth - Force a specific port to be unconditionally unauthorized.
auto - The controlled port will reflect the outcome of authentication.
force_auth - Force a specific port to be unconditionally authorized.

quiet_period - (Optional) It is the initialization value of the 'quietWhile' timer. The default value is 60 seconds and can be any value among 0 to 65535.
<sec 0-65535> - Enter the quiet period value here. This value must be between 0 and 65535 seconds.

tx_period - (Optional) It is the initialization value of the transmit timer period. The default value is 30 seconds and can be any integer value among 1 to 65535.
<sec 1-65535> - Enter the Tx period value here. This value must be between 1 and 65535 seconds.

supp_timeout - (Optional) The initialization value of the 'aWhile' timer when timing out the supplicant. Its default value is 30 seconds and can be any integer value among 1 to 65535.
<sec 1-65535> - Enter the supplicant timeout value here. This value must be between 1 and 65535 seconds.

server_timeout - (Optional) The initialization value of the aWhile timer when timing out the authentication server. Its default value is 30 seconds and can be any integer value among 1 to 65535.
<sec 1-65535> - Enter the server timeout value here. This value must be between 1 and 65535 seconds.

max_req - (Optional) The maximum number of times that the authentication PAE state machine will retransmit an EAP Request packet to the supplicant. Its default value is 2 and can be any integer number among 1 to 10.
<value 1-10> - Enter the maximum required value here. This value must be between 1 and 10.

reauth_period - (Optional) It's a nonzero number of seconds, which is used to be the re-authentication timer. The default value is 3600.
<sec 1-65535> - Enter the re-authentication period value here. This value must be between 1 and 65535 seconds.

enable_reauth - (Optional) You can enable or disable the re-authentication mechanism for a specific port.
enable - Specifies to enable the re-authentication mechanism for a specific port.
disable - Specifies to disable the re-authentication mechanism for a specific port.

max_users - (Optional) Specifies per port maximum number of users. The default value is 16.
<value 1-448> - Enter the maximum users value here. This value must be between 1 and 448.
no_limit - Specifies that no limit is enforced on the maximum users used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the parameters that control the operation of the authenticator associated with a port:

```
DWS-3160-24PC:admin# config 802.1x auth_parameter ports 1-20 direction both
Command: config 802.1x auth_parameter ports 1-20 direction both

Success.

DWS-3160-24PC:admin#
```

4-14 config 802.1x auth_mode

Description

This command is used to configure the 802.1X authentication mode.

Format

config 802.1x auth_mode [port_based | mac_based]

Parameters

port_based - Configure the authentication as port based mode.

mac_based - Configure the authentication as MAC based mode.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the 802.1X authentication mode:

```
DWS-3160-24PC:admin# config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based

Success.

DWS-3160-24PC:admin#
```

4-15 config 802.1x init

Description

This command is used to initialize the authentication state machine of some or all ports.

Format

config 802.1x init [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]

Parameters

port_based - Configure the authentication as port based mode.
  <portlist> - Enter the list of ports used for the configuration here.

all - Specifies that all ports will be used.

mac_based - Configure the authentication as MAC based mode.
<portlist> - Enter the list of ports used for the configuration here.
all - Specifies that all ports will be used.

mac_address - (Optional) Specifies the MAC address of client.
<macaddr> - Enter the MAC address used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To initialize the authentication state machine on all the ports:

```
DWS-3160-24PC:admin# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DWS-3160-24PC:admin#
```

4-16 config 802.1x reauth

Description

This command is used to re-authenticate the device connected to the port. During the re-authentication period, the port status will remain authorized until re-authentication failed.

Format

config 802.1x reauth [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]

Parameters

port_based - Configure the authentication as port based mode.
<portlist> - Enter the list of ports used for the configuration here.
all - Specifies that all ports will be used.

mac_based - Configure the authentication as MAC based mode.
<portlist> - Enter the list of ports used for the configuration here.
all - Specifies that all ports will be used.

mac_address - (Optional) Specifies the MAC address of client.
<macaddr> - Enter the MAC address used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To re-authenticate the device connected to the port:

```
DWS-3160-24PC:admin# config 802.1x reauth port_based ports all
Command: config 802.1x reauth port_based ports all

Success.

DWS-3160-24PC:admin#
```

4-17 create 802.1x guest_vlan

Description

This command is used to assign a static VLAN to be a guest VLAN. The specific VLAN which is assigned to the guest VLAN must already exist. When a specific VLAN is assigned to a guest VLAN, it cannot be delete.

Format

create 802.1x guest_vlan {<vlan_name 32>}

Parameters

guest_vlan - Specifies the VLAN to be guest VLAN.

<vlan_name 32> - (Optional) Enter the VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To assign a static VLAN, called ‘guestVLAN’, to be a guest VLAN:

```
DWS-3160-24PC:admin# create 802.1x guest_vlan guestVLAN
Command: create 802.1x guest_vlan guestVLAN

Success.

DWS-3160-24PC:admin#
```

4-18 delete 802.1x guest_vlan

Description

This command is used to delete a guest VLAN. This option will not delete the static VLAN. All enabled ports of the guest VLAN will be reassigned to their original VLAN after the guest VLAN was deleted.

Format

delete 802.1x guest_vlan {<vlan_name 32>}

Parameters

guest_vlan - Specifies the static VLAN to be guest VLAN.
<vlan_name 32> - (Optional) Enter the VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the guest VLAN called “guestVLAN”:

```
DWS-3160-24PC:admin# delete 802.1x guest_vlan guestVLAN
Command: delete 802.1x guest_vlan guestVLAN

Success.

DWS-3160-24PC:admin#
```

4-19 config 802.1x guest_vlan

Description

This command is used to configure a guest VLAN. If the specific port state is changed from enabled to disabled, this port will then be reassigned to its original VLAN.

Format

config 802.1x guest_vlan ports [<portlist> | all] state [enable | disable]

Parameters

ports - A range of ports enable or disable guest VLAN function.
<portlist> - Enter the list of ports used for the configuration here.
all - Specifies that all the port will be included in this configuration.

state - Specifies the guest VLAN port state of the configured ports.
enable - Specifies to join the guest VLAN.
disable - Specifies to be removed from the guest VLAN.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable ports 1 to 8, used be the guest VLAN:

```
DWS-3160-24PC:admin# config 802.1x guest_vlan ports 1-8 state enable
Command: config 802.1x guest_vlan ports 1-8 state enable

Warning! GVRP of the ports were disabled!

Success.

DWS-3160-24PC:admin#
```

4-20 show 802.1x guest_vlan

Description

This command is used to display the information of guest VLANs.

Format

show 802.1x guest_vlan

Parameters

None.

Restrictions

None.

Example

To display the information of a guest VLAN:

```
DWS-3160-24PC:admin#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Setting
-----------------------------------------------------------
Guest VLAN : guestVLAN
Enabled Guest VLAN Ports : 1-8

DWS-3160-24PC:admin#
```

4-21 config radius add

Description

This command is used to add a new RADIUS server. The RADIUS server with a lower index value will have a higher authenticate priority.

Format

config radius add <server_index 1-3> [<server_ip> | <ipv6addr>] key <password 32> [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <sec 1-255> | retransmit <int 1-20>}]

Parameters

add - Specifies to add a new RADIUS server.
<server_index 1-3> - Enter the RADIUS server index here. This value must be between 1 and 3.
<server_ip> - Enter the IP address of the RADIUS server here.
<ipv6addr> - Enter the IPv6 address of the RADIUS server here.

key - The key pre-negotiated between Switch and the RADIUS server. It is used to encrypt user's authentication data before being transmitted over internet. The maximum length of the key is 32.
<password 32> - Enter the password here. The password can be up to 32 characters long.

default - Sets the authentication UDP port number to 1812 accounting UDP port number to 1813, timeout to 5 seconds and retransmit to 2.

auth_port - (Optional) Specifies the UDP port number which is used to transmit RADIUS authentication data between the Switch and the RADIUS server. The range is 1 to 65535.
<udp_port_number 1-65535> - Enter the authentication port number here. This value must be between 1 and 65535.

acct_port - (Optional) Specifies the UDP port number which is used to transmit RADIUS accounting statistics between the Switch and the RADIUS server. The range is 1 to 65535.
<udp_port_number 1-65535> - Enter the accounting port number here. This value must be between 1 and 65535.

timeout - (Optional) The time in second for waiting server reply. The default value is 5 seconds.
<sec 1-255> - Enter the timeout value here. This value must be between 1 and 255 seconds.

retransmit - (Optional) The count for re-transmitting. The default value is 2.
<int 1-20> - Enter the re-transmit value here. This value must be between 1 and 20.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a new RADIUS server:

```
DWS-3160-24PC:admin# config radius add 1 10.48.74.121 key dlink default
Command: config radius add 1 10.48.74.121 key dlink default

Success.

DWS-3160-24PC:admin#
```

4-22 config radius delete

Description

This command is used to delete a RADIUS server.

Format

config radius delete <server_index 1-3>

Parameters

delete - Specifies to delete a RADIUS server.
<server_index 1-3> - Enter the RADIUS server index here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a RADIUS server:

```
DWS-3160-24PC:admin# config radius delete 1
Command: config radius delete 1

Success.

DWS-3160-24PC:admin#
```

4-23 config radius

Description

This command is used to configure a RADIUS server.

Format

config radius <server_index 1-3> {ipaddress [<server_ip> | <ipv6addr>] | key <password 32> | auth_port [<udp_port_number 1-65535> | default] | acct_port [<udp_port_number 1-65535> | default] | timeout [<sec 1-255> | default] | retransmit [<int 1-20> | default]}

Parameters

<server_index 1-3> - Enter the RADIUS server index here. This value must be between 1 and 3.

ipaddress - (Optional) The IP address of the RADIUS server.
<server_ip> - Enter the RADIUS server IP address here.
<ipv6addr> - Enter the RADIUS server IPv6 address used here.

key - (Optional) The key pre-negotiated between Switch and RADIUS server. It is used to encrypt user's authentication data before being transmitted over internet. The maximum length of the key is 32.
<password 32> - Enter the key here. The key can be up to 32 characters long.

auth_port - (Optional) Specifies the UDP port number which is used to transmit RADIUS authentication data between the Switch and the RADIUS server. The range is 1 to 65535. The default value is 1812.
<udp_port_number 1-65535> - Enter the authentication port number here. This value must be between 1 and 65535.
default - Specifies that the default port number will be used.

acct_port - (Optional) Specifies the UDP port number which is used to transmit RADIUS accounting statistics between the Switch and the RADIUS server. The range is 1 to 65535. The default value is 1813.

<udp_port_number 1-65535> - Enter the accounting port number here. This value must be between 1 and 65535.
default - Specifies that the default port number will be used.

timeout - (Optional) The time in second for waiting server reply. The default value is 5 seconds.
<sec 1-255> - Enter the timeout value here. This value must be between 1 and 255 seconds.
default - Specifies that the default timeout value will be used.

retransmit - (Optional) The count for re-transmitting. The default value is 2.
<int 1-20> - Enter the re-transmit value here. This value must be between 1 and 20.
default - Specifies that the default re-transmit value will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a RADIUS server:

```
DWS-3160-24PC:admin# config radius 1 auth_port 60
Command: config radius 1 auth_port 60

Success.

DWS-3160-24PC:admin#
```

4-24 show radius

Description

This command is used to display RADIUS server configurations.

Format

show radius

Parameters

None.

Restrictions

None.

Example

To display RADIUS server configurations:

```
DWS-3160-24PC:admin#show radius
Command: show radius

Index 1
    IP Address     : 10.48.74.121
    Auth-Port      : 60
    Acct-Port      : 1813
    Timeout        : 5
    Retransmit     : 2
    Key            : dlink

Total Entries : 1

DWS-3160-24PC:admin#
```

4-25 show auth_statistics

Description

This command is used to display information of authenticator statistics.

Format

show auth_statistics {ports <portlist>}

Parameters

ports - (Optional) Specifies a range of ports to be displayed.
<portlist> - Enter the list of ports that will be displayed here.

Restrictions

None.

Example

To display authenticator statistics information for port 1:

```
DWS-3160-24PC:admin# show auth_statistics ports 1
Command: show auth_statistics ports 1

Port Number : 1

 EapolFramesRx                       0
 EapolFramesTx                       0
 EapolStartFramesRx                  0
 EapolReqIdFramesTx                  0
 EapolLogoffFramesRx                 0
 EapolReqFramesTx                    0
 EapolRespIdFramesRx                 0
 EapolRespFramesRx                   0
 InvalidEapolFramesRx                0
 EapLengthErrorFramesRx              0

 LastEapolFrameVersion               0
 LastEapolFrameSource                00-00-00-00-00-00

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

4-26 show auth_diagnostics

Description

This command is used to display information of authenticator diagnostics.

Format

show auth_diagnostics {ports <portlist>}

Parameters

ports - (Optional) Specifies a range of ports to be displayed.
<portlist> - Enter the list of ports that will be displayed here.

Restrictions

None.

Example

To display authenticator diagnostics information for port 1:

```
DWS-3160-24PC:admin# show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1

Port Number: 1

 EntersConnecting                      0
 EapLogoffsWhileConnecting             0
 EntersAuthenticating                  0
 SuccessWhileAuthenticating            0
 TimeoutsWhileAuthenticating           0
 FailWhileAuthenticating               0
 ReauthsWhileAuthenticating            0
 EapStartsWhileAuthenticating          0
 EapLogoffWhileAuthenticating          0
 ReauthsWhileAuthenticated             0
 EapStartsWhileAuthenticated           0
 EapLogoffWhileAuthenticated           0
 BackendResponses                      0
 BackendAccessChallenges               0
 BackendOtherRequestsToSupplicant      0
 BackendNonNakResponsesFromSupplicant  0
 BackendAuthSuccesses                  0
 BackendAuthFails                      0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

4-27 show auth_session_statistics

Description

This command is used to display information of authenticator session statistics.

Format

show auth_session_statistics {ports <portlist>}

Parameters

ports - (Optional) Specifies a range of ports to be displayed.
<portlist> - Enter the list of ports that will be displayed here.

Restrictions

None.

Example

To display authenticator session statistics information for port 1:

```
DWS-3160-24PC:admin# show auth_session_statistics ports 1
Command: show auth_session_statistics ports 1

Port Number : 1

 SessionOctetsRx                  0
 SessionOctetsTx                  0
 SessionFramesRx                  0
 SessionFramesTx                  0
 SessionId
 SessionAuthenticMethod           Remote Authentication Server
 SessionTime                      0
 SessionTerminateCause            SupplicantLogoff
 SessionUserName

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

4-28 show auth_client

Description

This command is used to display information of RADIUS authentication client.

Format

show auth_client

Parameters

None.

Restrictions

None.

Example

To display authentication client information:

```
DWS-3160-24PC:admin# show auth_client
Command: show auth_client

 radiusAuthClient ==>
 radiusAuthClientInvalidServerAddresses   0
 radiusAuthClientIdentifier

 radiusAuthServerEntry ==>
 radiusAuthServerIndex :1

 radiusAuthServerAddress                  10.48.74.121
 radiusAuthClientServerPortNumber         60
 radiusAuthClientRoundTripTime            0
 radiusAuthClientAccessRequests           0
 radiusAuthClientAccessRetransmissions    0
 radiusAuthClientAccessAccepts            0
 radiusAuthClientAccessRejects            0
 radiusAuthClientAccessChallenges         0
 radiusAuthClientMalformedAccessResponses 0
 radiusAuthClientBadAuthenticators        0
 radiusAuthClientPendingRequests          0
 radiusAuthClientTimeouts                 0
 radiusAuthClientUnknownTypes             0
 radiusAuthClientPacketsDropped           0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

4-29 show acct_client

Description

This command is used to display information of RADIUS accounting client.

Format

show acct_client

Parameters

None.

Restrictions

None.

Example

To display information of RADIUS accounting client:

```
DWS-3160-24PC:admin# show acct_client
Command: show acct_client

 radiusAcctClient ==>
 radiusAcctClientInvalidServerAddresses   0
 radiusAcctClientIdentifier

 radiusAuthServerEntry ==>
 radiusAccServerIndex : 1

 radiusAccServerAddress                   10.48.74.121
 radiusAccClientServerPortNumber          1813
 radiusAccClientRoundTripTime             0
 radiusAccClientRequests                  0
 radiusAccClientRetransmissions           0
 radiusAccClientResponses                 0
 radiusAccClientMalformedResponses        0
 radiusAccClientBadAuthenticators         0
 radiusAccClientPendingRequests           0
 radiusAccClientTimeouts                  0
 radiusAccClientUnknownTypes              0
 radiusAccClientPacketsDropped            0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

4-30 config accounting service

Description

This command is used to configure the state of the specified RADIUS accounting service.

Format

config accounting service [network | shell | system] state [enable | disable]

Parameters

network - Accounting service for 802.1X port access control. By default, the service is disabled.

shell - Accounting service for shell events: When user logs on or out the Switch (via the console, TELNET, or SSH) and timeout occurs, accounting information will be collected and sent to RADIUS server. By default, the service is disabled.

system - Accounting service for system events: reset, reboot. By default, the service is disabled.

state - Specifies the state of the specified service.

enable - Specifies to enable the specified accounting service.

disable - Specifies to disable the specified accounting service.

Restrictions

Only Administrators and Operators can issue this command.

Example

Enable it to configure accounting shell state:

```
DWS-3160-24PC:admin# config accounting service shell state enable
Command: config accounting service shell state enable

Success.

DWS-3160-24PC:admin#
```

4-31 show accounting service

Description

This command is used to display the status of RADIUS accounting services.

Format

show accounting service

Parameters

None.

Restrictions

None.

Example

To display information of RADIUS accounting services:

```
DWS-3160-24PC:admin#show accounting service
Command: show accounting service

Accounting State
-------------------
Network : Disabled
Shell   : Enabled
System  : Disabled

DWS-3160-24PC:admin#
```

Chapter 5 Access Authentication Control Command List

enable password encryption

disable password encryption

enable authen_policy

disable authen_policy

show authen_policy

create authen_login method_list_name <string 15>

config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}

delete authen_login method_list_name <string 15>

show authen_login [default | method_list_name <string 15> | all]

create authen_enable method_list_name <string 15>

config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local _enable | none}

delete authen_enable method_list_name <string 15>

show authen_enable [default | method_list_name <string 15> | all]

config authen application [console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]

show authen application

create authen server_group <string 15>

config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]

delete authen server_group <string 15>

show authen server_group {<string 15>}

create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] { port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20> }

config authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+| radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}

delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]

show authen server_host

config authen parameter response_timeout <int 0-255>

config authen parameter attempt <int 1-255>

show authen parameter

enable admin

config admin local_enable

5-1 enable password encryption

Description

This command is used to enable password encryption. The user account configuration information will be stored in the configuration file, and can be applied to the system later.

If the password encryption is enabled, the password will be in encrypted form.

Format

enable password encryption

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the password encryption:

```
DWS-3160-24PC:admin# enable password encryption
Command: enable password encryption

DWS-3160-24PC:admin#
```

5-2 disable password encryption

Description

This command is used to disable password encryption. The user account configuration information will be stored in the configuration file, and can be applied to the system later.

When password encryption is disabled, if the user specifies the password in plain text form, the password will be in plain text form. However, if the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enable password encryption command, the password will still be in the encrypted form. It cannot be reverted to the plaintext.

Format

disable password encryption

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the password encryption:

```
DWS-3160-24PC:admin# disable password encryption
Command: disable password encryption

DWS-3160-24PC:admin#
```

5-3 enable authen_policy

Description

This command is used to enable system access authentication policy.

Enable system access authentication policy. When authentication is enabled, the device will adopt the login authentication method list to authenticate the user for login, and adopt the enable authentication method list to authenticate the enable password for promoting the user‘s privilege to Admin level.

Format

enable authen_policy

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable system access authentication policy:

```
DWS-3160-24PC:admin# enable authen_policy
Command: enable authen_policy

Success.

DWS-3160-24PC:admin#
```

5-4 disable authen_policy

Description

This command is used to disable system access authentication policy.

Disable system access authentication policy. When authentication is disabled, the device will adopt the local user account database to authenticate the user for login, and adopt the local enable password to authenticate the enable password for promoting the user‘s privilege to Admin level.

Format

disable authen_policy

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable system access authentication policy:

```
DWS-3160-24PC:admin# disable authen_policy
Command: disable authen_policy

Success.

DWS-3160-24PC:admin#
```

5-5 show authen_policy

Description

This command is used to display that system access authentication policy is enabled or disabled.

Format

show authen_policy

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display system access authentication policy:

```
DWS-3160-24PC:admin#show authen_policy
Command: show authen_policy

Authentication Policy : Enabled

DWS-3160-24PC:admin#
```

5-6 create authen_login

Description

This command is used to create a user-defined method list of authentication methods for user login. The maximum supported number of the login method lists is 8.

Format

create authen_login method_list_name <string 15>

Parameters

<string 15> - The user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create a user-defined method list for user login:

```
DWS-3160-24PC:admin# create authen_login method_list_name login_list_1
Command: create authen_login method_list_name login_list_1

Success.

DWS-3160-24PC:admin#
```

5-7 config authen_login

Description

This command is used to configure a user-defined or default method list of authentication methods for user login. The sequence of methods will affect the altercation result. For example, if the sequence is TACACS+ first, then TACACS and local, when user tries to login, the authentication request will be sent to the first server host in TACACS+ built-in server group. If the first server host in TACACS+ group is missing, the authentication request will be sent to the second server host in TACACS+ group, and so on. If all server hosts in TACACS+ group are missing, the authentication request will be sent to the first server host in TACACS group. If all server hosts in TACACS group are missing, the local account database in the device is used to authenticate this user. When user logins the device successfully while using methods like TACACS/XTACACS/TACACS+/RADIUS built-in or user-defined server groups or none, the "user" privilege level is assigned only. If user wants to get admin privilege level, user must use the "enable admin" command to promote his privilege level. But when local method is used, the privilege level will depend on this account privilege level stored in the local device.

Format

config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}

Parameters

default - The default method list of authentication methods.
method_list_name - The user-defined method list of authentication methods. **<string 15> -** Enter the method list name here. This value can be up to 15 characters long.
method - Specifies the authentication method used. **tacacs** - (Optional) Authentication by the built-in server group "TACACS".

xtacacs - (Optional) Authentication by the built-in server group “XTACACS”.
tacacs+ - (Optional) Authentication by the built-in server group “TACACS+”.
radius - (Optional) Authentication by the built-in server group “RADIUS”.
server_group - (Optional) Authentication by the user-defined server group.
<string 15> - Enter the server group value here. This value can be up 15 characters long.
local - (Optional) Authentication by local user account database in device.
none - (Optional) No authentication.

Restrictions

Only Administrators can issue this command.

Example

To configure a user-defined method list for user login:

```
DWS-3160-24PC:admin# config authen_login method_list_name login_list_1 method
tacacs+ tacacs local
Command: config authen_login method_list_name login_list_1 method tacacs+
tacacs local

Success.

DWS-3160-24PC:admin#
```

5-8 delete authen_login

Description

This command is used to delete a user-defined method list of authentication methods for user login.

Format

delete authen_login method_list_name <string 15>

Parameters

<string 15> - The user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a user-defined method list for user login:

```
DWS-3160-24PC:admin# delete authen_login method_list_name login_list_1
Command: delete authen_login method_list_name login_list_1

Success.

DWS-3160-24PC:admin#
```

5-9 show authen_login

Description

This command is used to display the method list of authentication methods for user login.

Format

show authen_login [default | method_list_name <string 15> | all]

Parameters

default - Display default user-defined method list for user login.

method_list_name - Display the specific user-defined method list for user login.
<string 15> - Enter the method list name here. This value can be up to 15 characters long.

all - Display all method lists for user login.

Restrictions

Only Administrators can issue this command.

Example

To display a user-defined method list for user login:

```
DWS-3160-24PC:admin# show authen_login method_list_name login_list_1
Command: show authen_login method_list_name login_list_1

Method List Name  Priority  Method Name      Comment
----------------  --------  ---------------  ------------------
login_list_1      1         tacacs+          Built-in Group
                  2         tacacs           Built-in Group
                  3         mix_1            User-defined Group
                  4         local            Keyword

DWS-3160-24PC:admin#
```

5-10 create authen_enable

Description

This command is used to create a user-defined method list of authentication methods for promoting user's privilege to Admin level.

Format

create authen_enable method_list_name <string 15>

Parameters

<string 15> - The user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create a user-defined method list for promoting user's privilege to Admin level:

```
DWS-3160-24PC:admin# create authen_enable method_list_name enable_list_1
Command: create authen_enable method_list_name enable_list_1

Success.

DWS-3160-24PC:admin#
```

5-11 config authen_enable

Description

This command is used to configure a user-defined or default method list of authentication methods for promoting user's privilege to Admin level. The sequence of methods will affect the altercation result. For example, if the sequence is TACACS+ first, then TACACS and local_enable, when user try to promote user's privilege to Admin level, the authentication request will be sent to the first server host in TACACS+ built-in server group. If the first server host in TACACS+ group is missing, the authentication request will be sent to the second server host in TACACS+ group, and so on. If all server hosts in TACACS+ group are missing, the authentication request will be sent to the first server host in TACACS group…If all server hosts in TACACS group are missing, the local enable password in the device is used to authenticate this user’s password.

Format

config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local _enable | none}

Parameters

default - The default method list of authentication methods.

method_list_name - The user-defined method list of authentication methods.
  <string 15> Enter the method list name here. This value can be up to 15 characters long.

method - Specifies the authentication method used.
  tacacs - (Optional) Authentication by the built-in server group “TACACS”.
  xtacacs - (Optional) Authentication by the built-in server group “XTACACS”.
  tacacs+ - (Optional) Authentication by the built-in server group “TACACS+”.
  radius - (Optional) Authentication by the built-in server group “RADIUS”.
  server_group - (Optional) Authentication by the user-defined server group.
    <string 15> - Enter the server group name here. This value can be up to 15 characters long.
  local_enable - (Optional) Authentication by local enable password in device.
  none - (Optional) No authentication.

Restrictions

Only Administrators can issue this command.

Example

To configure a user-defined method list for promoting user's privilege to Admin level:

```
DWS-3160-24PC:admin# config authen_enable method_list_name enable_list_1 method
tacacs+ tacacs local_enable
Command: config authen_ enable method_list_name enable_list_1 method tacacs+
tacacs local_enable

Success.

DWS-3160-24PC:admin#
```

5-12 delete authen_enable

Description

This command is used to delete a user-defined method list of authentication methods for promoting user's privilege to Admin level.

Format

delete authen_enable method_list_name <string 15>

Parameters

<string 15> - The user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a user-defined method list for promoting user's privilege to Admin level:

```
DWS-3160-24PC:admin# delete authen_enable method_list_name enable_list_1
Command: delete authen_enable method_list_name enable_list_1

Success.

DWS-3160-24PC:admin#
```

5-13 show authen_enable

Description

This command is used to display the method list of authentication methods for promoting user's privilege to Admin level.

Format

show authen_enable [default | method_list_name <string 15> | all]

Parameters

default - Display default user-defined method list for promoting user's privilege to Admin level.

method_list_name - Display the specific user-defined method list for promoting user's privilege to Admin level.
<string 15> - Enter the method list name here. This value can be up to 15 characters long.

all - Display all method lists for promoting user's privilege to Admin level.

Restrictions

Only Administrators can issue this command.

Example

To display all method lists for promoting user's privilege to Admin level:

```
DWS-3160-24PC:admin#show authen_enable method_list_name enable_list_1
Command: show authen_enable method_list_name enable_list_1

Method List Name  Priority  Method Name      Comment
----------------  --------  ---------------  ------------------
enable_list_1             1         tacacs+          Built-in Group
                          2         tacacs           Built-in Group
                          3         mix_1            User-defined Group
                          4         local            Keyword

Total Entries : 1

DWS-3160-24PC:admin#
```

5-14 config authen application

Description

This command is used to configure login or enable method list for all or the specified application.

Format

config authen application [console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]

Parameters

console - Application: console.
telnet - Application: TELNET.
ssh - Application: SSH.
http - Application: web.
all - Application: console, TELNET, SSH, and web.

login - Select the method list of authentication methods for user login.
enable - Select the method list of authentication methods for promoting user's privilege to Admin level.

default - Default method list.
method_list_name - The user-defined method list name.

<string> - Enter the method list name here. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To configure the login method list for TELNET:

```
DWS-3160-24PC:admin# config authen application telnet login method_list_name
login_list_1
Command: config authen application telnet login method_list_name login_list_1

Success.

DWS-3160-24PC:admin#
```

5-15 show authen application

Description

This command is used to display the login/enable method list for all applications.

Format

show authen application

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display the login/enable method list for all applications:

```
DWS-3160-24PC:admin#show authen application
Command: show authen application

Application  Login Method List  Enable Method List
-----------  -----------------  ------------------
Console      default            default
Telnet       login_list_1       default
SSH          default            default
HTTP         default            default

DWS-3160-24PC:admin#
```

5-16 create authen server_group

Description

This command is used to create a user-defined authentication server group. The maximum supported number of server groups including built-in server groups is 8. Each group consists of 8 server hosts as maximum.

Format

create authen server_group <string 15>

Parameters

<string 15> - The user-defined server group name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create a user-defined authentication server group:

```
DWS-3160-24PC:admin# create authen server_group mix_1
Command: create authen server_group mix_1

Success.

DWS-3160-24PC:admin#
```

5-17 config authen server_group

Description

This command is used to add or remove an authentication server host to or from the specified server group. Built-in server group “TACACS”, “XTACACS”, “TACACS+”, “RADIUS” accepts the server host with the same protocol only, but user-defined server group can accept server hosts with different protocols.

Format

config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]

Parameters

server_group - User-defined server group.

- **tacacs** - Built-in server group “TACACS”.
- **xtacacs** - Built-in server group “XTACACS”.
- **tacacs+** - Built-in server group “TACACS+”.
- **radius** - Built-in server group “RADIUS”.
- **<string 15>** - Enter the server group name here. This value can be up to 15 characters long.

add - Add a server host to a server group. **delete** - Remove a server host from a server group.
server_host - Server host's IP address. **<ipaddr>** - Enter the server host IP address here.
protocol - Specifies the authentication protocol used. **tacacs** - Specifies that the TACACS authentication protocol will be used. **xtacacs** - Specifies that the XTACACS authentication protocol will be used. **tacacs+** - Specifies that the TACACS+ authentication protocol will be used. **radius** - Specifies that the RADIUS authentication protocol will be used.

Restrictions

Only Administrators can issue this command.

Example

To add an authentication server host to an server group:

```
DWS-3160-24PC:admin# config authen server_group mix_1 add server_host
10.1.1.222 protocol tacacs+
Command: config authen server_group mix_1 add server_host 10.1.1.222 protocol
tacacs+

Success.

DWS-3160-24PC:admin#
```

5-18 delete authen server_group

Description

This command is used to delete a user-defined authentication server group.

Format

delete authen server_group <string 15>

Parameters

<string 15> - The user-defined server group name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a user-defined authentication server group:

```
DWS-3160-24PC:admin# delete authen server_group mix_1
Command: delete authen server_group mix_1

Success.

DWS-3160-24PC:admin#
```

5-19 show authen server_group

Description

This command is used to display the authentication server groups.

Format

show authen server_group {<string 15>}

Parameters

<string 15> - (Optional) The built-in or user-defined server group name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To display all authentication server groups:

```
DWS-3160-24PC:admin# show authen server_group
Command: show authen server_group

Group Name       IP Address       Protocol
---------------  ---------------  --------
mix_1            10.1.1.222       TACACS+
                 10.1.1.223       TACACS
radius           10.1.1.224       RADIUS
tacacs           10.1.1.225       TACACS
tacacs+          10.1.1.226       TACACS+
xtacacs          10.1.1.227       XTACACS

Total Entries : 5

DWS-3160-24PC:admin#
```

5-20 create authen server_host

Description

This command is used to create an authentication server host. When an authentication server host is created, IP address and protocol are the index. That means over 1 authentication protocol services can be run on the same physical host. The maximum supported number of server hosts is 16.

Format

create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] { port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20> }

Parameters

server_host - Server host's IP address.
<ipaddr> - Enter the server host IP address used here.

protocol - Specifies the host's authentication protocol.
tacacs - Server host's authentication protocol.
xtacacs - Server host's authentication protocol.
tacacs+ - Server host's authentication protocol.
radius - Server host's authentication protocol.

port - (Optional) The port number of authentication protocol for server host. Default value for TACACS/XTACACS/TACACS+ is 49. Default value for RADIUS is 1812.
<int 1-65535> - Enter the authentication protocol port number here. This value must be between 1 and 65535.

key - (Optional) The key for TACACS+ and RADIUS authentication. If the value is null, no encryption will apply. This value is meaningless for TACACS and XTACACS.
<key_string 254> - Enter the TACACS+ or the RADIUS key here. This key can be up to 254 characters long.
none - No encryption for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS.

timeout - (Optional) The time in second for waiting server reply. Default value is 5 seconds.
<int 1-255> - Enter the timeout value here. This value must be between 1 and 255 seconds.

retransmit - (Optional) The count for re-transmit. This value is meaningless for TACACS+. Default value is 2.
<int 1-20> - Enter the re-transmit value here. This value must be between 1 and 20.

Restrictions

Only Administrators can issue this command.

Example

To create a TACACS+ authentication server host, its listening port number is 15555 and timeout value is 10 seconds:

```
DWS-3160-24PC:admin# create authen server_host 10.1.1.222 protocol tacacs+ port
15555 timeout 10
Command: create authen server_host 10.1.1.222 protocol tacacs+ port 15555
timeout 10


Success.


DWS-3160-24PC:admin#
```

5-21 config authen server_host

Description

This command is used to configure an authentication server host.

Format

config authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}

Parameters

server_host - Server host’s IP address.
  <ipaddr> - Enter the server host IP address here.

protocol - Specifies the server host's authentication protocol.
  tacacs - Server host’s authentication protocol.
  xtacacs - Server host’s authentication protocol.
  tacacs+ - Server host’s authentication protocol.
  radius - Server host’s authentication protocol.

port - (Optional) The port number of authentication protocol for server host. Default value for TACACS/XTACACS/TACACS+ is 49. Default value for RADIUS is 1812.
  <int 1-65535> - Enter the port number here. This value must be between 1 and 65535.

key - (Optional) The key for TACACS+ and RADIUS authentication. If the value is null, no encryption will apply. This value is meaningless for TACACS and XTACACS.
  <key_string 254> - Enter the TACACS+ key here. This value can be up to 254 characters long.
  none - No encryption for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS.

timeout - (Optional) The time in second for waiting server reply. Default value is 5 seconds.
  <int 1-255> - Enter the timeout value here. This value must be between 1 and 255 seconds.

retransmit - (Optional) The count for re-transmit. This value is meaningless for TACACS+. Default value is 2.
  <int 1-20> - Enter the re-transmit value here. This value must be between 1 and 20.

Restrictions

Only Administrators can issue this command.

Example

To configure a TACACS+ authentication server host’s key value:

```
DWS-3160-24PC:admin# config authen server_host 10.1.1.222 protocol tacacs+ key
"This is a secret"
Command: config authen server_host 10.1.1.222 protocol tacacs+ key "This is a
secret"

Success.

DWS-3160-24PC:admin#
```

5-22 delete authen server_host

Description

This command is used to delete an authentication server host.

Format

delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]

Parameters

server_host - Server host’s IP address.
  <ipaddr> - Enter the server host's IP address here.

protocol - Specifies that server host's authentication protocol.
  tacacs - Server host’s authentication protocol.
  xtacacs - Server host’s authentication protocol.
  tacacs+ - Server host’s authentication protocol.
  radius - Server host’s authentication protocol.

Restrictions

Only Administrators can issue this command.

Example

To delete an authentication server host:

```
DWS-3160-24PC:admin# delete authen server_host 10.1.1.222 protocol tacacs+
Command: delete authen server_host 10.1.1.222 protocol tacacs+

Success.

DWS-3160-24PC:admin#
```

5-23 show authen server_host

Description

This command is used to display the authentication server hosts.

Format

show authen server_host

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display all authentication server hosts:

```
DWS-3160-24PC:admin#show authen server_host
Command: show authen server_host

IP Address       Protocol  Port   Timeout  Retransmit  Key
---------------  --------  -----  -------  ----------  ----------------------
10.1.1.222       TACACS+   49     5        ------      This is a secret

Total Entries : 1

DWS-3160-24PC:admin#
```

5-24 config authen parameter response_timeout

Description

This command is used to configure the amount of time waiting or user input on console, TELNET, SSH application.

Format

config authen parameter response_timeout <int 0-255>

Parameters

response_timeout - The amount of time for user input on console or TELNET or SSH. 0 means there is no time out. Default value is 30 seconds.

<int 0-255> - Enter the response timeout value here. This value must be between 0 and 255.

Restrictions

Only Administrators can issue this command.

Example

To configure the amount of time waiting or user input to be 60 seconds:

```
DWS-3160-24PC:admin# config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DWS-3160-24PC:admin#
```

5-25 config authen parameter attempt

Description

This command is used to configure the maximum attempts for user's trying to login or promote the privilege on console, TELNET, SSH application.

Format

config authen parameter attempt <int 1-255>

Parameters

attempt - The amount of attempts for user's trying to login or promote the privilege on console or TELNET or SSH. Default value is 3.

<int 1-255> - Enter the attempt amount here. This value must be between 1 and 255.

Restrictions

Only Administrators can issue this command.

Example

To configure the maximum attempts for user's trying to login or promote the privilege to be 9:

```
DWS-3160-24PC:admin# config authen parameter attempt 9
Command: config authen parameter attempt 9

Success.

DWS-3160-24PC:admin#
```

5-26 show authen parameter

Description

This command is used to display the parameters of authentication.

Format

show authen parameter

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display the parameters of authentication:

```
DWS-3160-24PC:admin#show authen parameter
Command: show authen parameter

Response Timeout : 60 seconds
User Attempts    : 9

DWS-3160-24PC:admin#
```

5-27 enable admin

Description

This command is used to enter the administrator level privilege. Promote the "user" privilege level to "admin" level. When the user enters this command, the authentication method TACACS, XTACACS, TACACS+, user-defined server groups, local_enable or none will be used to authenticate the user. Because TACACS, XTACACS and RADIUS don't support "enable" function in itself, if user wants to use either one of these 3 protocols to do enable authentication, user must create a special account on the server host first, which has a username "enable" and then configure its password as the enable password to support "enable" function.

This command cannot be used when authentication policy is disabled.

Format

enable admin

Parameters

None.

Restrictions

None.

Example

To enable administrator lever privilege:

```
DWS-3160-24PC:user#enable admin
Command: enable admin

PassWord:*************************
Success.

DWS-3160-24PC:admin#
```

5-28 config admin local_enable

Description

This command is used to configure the local enable password of administrator level privilege. When the user chooses the “local_enable” method to promote the privilege level, the enable password of local device is needed. When the password information is not specified in the command, the system will prompt the user to input the password interactively. For this case, the user can only input the plain text password. If the password is present in the command, the user can select to input the password in the plain text form or in the encrypted form. The encryption algorithm is based on SHA-I.

Format

config admin local_enable

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To configure the administrator password:

```
DWS-3160-24PC:admin# config admin local_enable
Command: config admin local_ebable

Enter the old password:
Enter the case-sensitive new password:******
Enter the new password again for confirmation:******
Success.

DWS-3160-24PC:admin#
```

Chapter 6 Access Control List (ACL) Command List

create access_profile profile_id <value 1-6> profile_name <name 1-32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}]

delete access_profile [profile_id <value 1-6> | profile_name <name 1-32> | all]

config access_profile [profile_id <value 1-6> | profile_name <name 1-32>] [add access_id [auto_assign | <value 1-256>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]} | packet_content {offset_chunk_1 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_2 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_3 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_4 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}} | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> {mask<ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type <value 0-255> | code <value 0-255>}]}] [port [<portlist> | all] | vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]] [permit {priority <value 0-7> {replace_priority} | [replace_dscp_with <value 0-63> | replace_tos_precedence_with <value 0-7>] | counter [enable | disable]} | mirror | deny] {time_range <range_name 32>} | delete access_id <value 1-256>]

show access_profile {[profile_id <value 1-6> | profile_name <name 1-32>]}

config flow_meter [profile_id <value 1-6> | profile_name <name 1-32>] access_id <value 1-256> [rate [<value 0-1048576>] {burst_size [<value 0-131072>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 0-1048576> {cbs <value 0-131072>} pir <value 0-1048576> {pbs <value 0-131072>} {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | sr_tcm cir <value 0-1048576> cbs <value 0-131072> ebs <value 0-131072> {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | delete]

show flow_meter {[profile_id <value 1-6> | profile_name <name 1-32>] {access_id <value 1-256>}}

config time_range <range_name 32> [hours start_time <time hh:mm:ss> end_time <time

hh:mm:ss> weekdays <daylist> | delete]
show time_range
show current_config access_profile

6-1 create access_profile

Description

This command is used to create an access profile for access list rules.

Format

create access_profile profile_id <value 1-6> profile_name <name 1-32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}]

Parameters

profile_id - Specifies the index of the access list profile. **<value 1-6>** - Enter the profile ID here. This value must be between 1 and 6.
profile_name - The name of the profile must be specified. The maximum length is 32 characters. **<name 1-32>** - Enter the profile name here.
ethernet - Specifies this is an ethernet mask.
vlan - (Optional) Specifies a VLAN mask. Only the last 12 bits of the mask will be considered. **<hex 0x0-0x0fff>** - Enter the VLAN mask value here.
source_mac - (Optional) Specifies the source MAC mask. **<macmask>** - Enter the source MAC address used here.
destination_mac - (Optional) Specifies the destination MAC mask. **<macmask>** - Enter the destination MAC address used here.
802.1p - (Optional) Specifies the 802.1p priority tag mask.
ethernet_type - (Optional) Specifies the Ethernet type mask.
ip - Specifies this is a IPv4 mask.
vlan - (Optional) Specifies a VLAN mask. Only the last 12 bits of the mask will be considered. **<hex 0x0-0x0fff>** -Enter the VLAN mask value here.
source_ip_mask - (Optional) Specifies a source IP address mask. **<netmask>** - Enter the source IP address mask here.
destination_ip_mask - (Optional) Specifies a destination IP address mask. **<netmask>** - Enter the destination IP address mask here.
dscp - (Optional) Specifies the DSCP mask.
icmp - (Optional) Specifies that the rule applies to ICMP traffic. **type** - Specifies the type of ICMP traffic. **code** - Specifies the code of ICMP traffic
igmp - (Optional) Specifies that the rule applies to IGMP traffic. **type** - Specifies the type of IGMP traffic.

tcp - (Optional) Specifies that the rule applies to TCP traffic. **src_port_mask** - Specifies the TCP source port mask. **<hex 0x0-0xffff>** - Enter the TCP source port mask here. **dst_port_mask** - Specifies the TCP destination port mask. **<hex 0x0-0xffff>** - Enter the TCP destination port mask here.
flag_mask - (Optional) Specifies the TCP flag field mask. **all** – Specifies that all the flags will be used for the TCP mask. **urg** – Specifies that the TCP flag field will be set to 'urg'. **ack** - Specifies that the TCP flag field will be set to 'ack'. **psh** - Specifies that the TCP flag field will be set to 'psh'. **rst** - Specifies that the TCP flag field will be set to 'rst'. **syn** - Specifies that the TCP flag field will be set to 'syn'. **fin** - Specifies that the TCP flag field will be set to 'fin'.
udp - (Optional) Specifies that the rule applies to UDP traffic. **src_port_mask** - Specifies the UDP source port mask. **<hex 0x0-0xffff>** - Enter the UDP source port mask here. **dst_port_mask** - Specifies the UDP destination port mask. **<hex 0x0-0xffff>** - Enter the UDP destination port mask here.
protocol_id_mask - (Optional) Specifies that the rule applies to IP protocol ID traffic. **<0x0-0xff>** - Enter the protocol ID mask here.
user_define_mask - (Optional) Specifies that the rule applies to the IP protocol ID, and that the mask option behind the IP header length is 20 bytes. **<hex 0x0-0xffffffff>** - Enter a user-defined mask value here.
packet_content_mask - Specifies the packet content mask. Only one packet_content_mask profile can be created. **offset_chunk_1** - (Optional) Specifies that the offset chunk 1 will be used. **<value 0-31>** - Enter the offset chunk 1 value here. This value must be between 0 and 31. **<hex 0x0-0xffffffff>** - Enter the offset chunk 1 mask here. **offset_chunk_2** - (Optional) Specifies that the offset chunk 2 will be used. **<value 0-31>** - Enter the offset chunk 2 value here. This value must be between 0 and 31. **<hex 0x0-0xffffffff>** - Enter the offset chunk 2 mask here. **offset_chunk_3** - (Optional) Specifies that the offset chunk 3 will be used. **<value 0-31>** - Enter the offset chunk 3 value here. This value must be between 0 and 31. **<hex 0x0-0xffffffff>** - Enter the offset chunk 3 mask here. **offset_chunk_4** - (Optional) Specifies that the offset chunk 4 will be used. **<value 0-31>** - Enter the offset chunk 4 value here. This value must be between 0 and 31. **<hex 0x0-0xffffffff>** - Enter the offset chunk 4 mask here.
ipv6 - (Optional) Specifies this is the IPv6 mask.
class - (Optional) Specifies the IPv6 class.
flowlabel - (Optional) Specifies the IPv6 flow label.
source_ipv6_mask - (Optional) Specifies an IPv6 source sub-mask. **<ipv6mask>** - Enter the source IPv6 mask value here.
destination_ipv6_mask - (Optional) Specifies an IPv6 destination sub-mask. **<ipv6mask>** -Enter the destination IPv6 mask value here.
tcp - (Optional) Specifies that the rule applies to TCP traffic. **src_port_mask** - Specifies an IPv6 Layer 4 TCP source port mask. **<hex 0x0-0xffff>** - Enter the TCP source port mask value here. **des_port_mask** - Specifies an IPv6 Layer 4 TCP destination port mask. **<hex 0x0-0xffff>** - Enter the TCP destination port mask value here.
udp - (Optional) Specifies that the rule applies to UDP traffic. **src_port_mask** - Specifies the UDP source port mask. **<hex 0x0-0xffff>** - Enter the UDP source port mask value here. **dst_port_mask** - Specifies the UDP destination port mask. **<hex 0x0-0xffff>** - Enter the UDP destination port mask value here.
icmp - (Optional) Specifies a mask for ICMP filtering. **type** - Specifies the inclusion of the ICMP type field in the mask. **code** - Specifies the inclusion of the ICMP code field in the mask.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an access profile:

```
DWS-3160-24PC:admin# create access_profile profile_id 1 profile_name t1
ethernet vlan source_mac 00-00-00-00-00-01 destination_mac 00-00-00-00-00-02
802.1p ethernet_type
Command: create access_profile profile_id 1 profile_name 1 ethernet vlan
source_mac 00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p
ethernet_type

Success.

DWS-3160-24PC:admin# create access_profile profile_id 2 profile_name 2 ip vlan
source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type code
Command: create access_profile profile_id 2 profile_name t2 ip vlan
source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type code

Success.

DWS-3160-24PC:admin# create access_profile profile_id 4 profile_name 4
packet_content_mask offset_chunk_1 3 0xFFFF offset_chunk_2 5 0xFF00
offset_chunk_3 14 0xFFFF0000 offset_chunk_4 16 0xFF000000
Command: create access_profile profile_id 4 profile_name 4 packet_content_mask
offset_chunk_1 3 0xFFFF offset_chunk_2 5 0xFF00 offset_chunk_3 14 0xFFFF0000
offset_chunk_4 16 0xFF000000

Success.

DWS-3160-24PC:admin#
```

6-2 delete access_profile

Description

This command is used to delete an access profile.

Format

delete access_profile [profile_id <value 1-6> | profile_name <name 1-32> | all]

Parameters

profile_id - Specifies the index of the access list profile.
<value 1-6> - Enter the profile ID value here. This value must be between 1 and 6.

profile_name - Specifies the name of the profile. The maximum length is 32 characters.
<name 1-32> - Enter the profile name here. This value must be between 1 and 32.

all - Specifies that the whole access list profile will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the access list rule with a profile ID of 10:

```
DWS-3160-24PC:admin# delete access_profile profile_id 10
Command: delete access_profile profile_id 10

Success.

DWS-3160-24PC:admin#
```

6-3 config access_profile

Description

This command is used to configure an access list entry. The ACL mirror function works after the mirror has been enabled and the mirror port has been configured using the mirror command.

When applying an access rule to a target, the setting specified in the VLAN field will not take effect if the target is a VLAN.

Format

config access_profile [profile_id <value 1-6> | profile_name <name 1-32>] [add access_id [auto_assign | <value 1-256>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]]} | packet_content {offset_chunk_1 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_2 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_3 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_4 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}} | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> {mask<ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type <value 0-255> | code <value 0-255>}]}] [port [<portlist> | all] | vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]] [permit {priority <value 0-7> {replace_priority} | [replace_dscp_with <value 0-63> | replace_tos_precedence_with <value 0-7>] | counter [enable | disable]} | mirror | deny] {time_range <range_name 32>} | delete access_id <value 1-256>]

Parameters

profile_id - Specifies the index of the access list profile.
<value 1-6> - Enter the profile ID value here. This value must be between 1 and 6.

profile_name - Specifies the name of the profile.

<name 1-32> - Enter the profile name here. This name can be up to 32 characters long.

add - Specifies that a profile or a rule will be added.

access_id - Specifies the index of the access list entry. The value range is 1-256, but the supported maximum number of entries depends on the project. If the auto_assign option is selected, the access ID is automatically assigned, when adding multiple ports.
auto_assign - Specifies that the access ID will automatically be assigned.
<value 1-256> - Enter the access ID used here. This value must be between 1 and 256.

ethernet - Specifies to configure the ethernet access profile.

vlan - (Optional) Specifies the VLAN name.
<vlan_name 32> - Enter the name of the VLAN here. This name can be up to 32 characters long.
vlan_id - (Optional) Specifies the VLAN ID used.
<vlanid 1-4094> - Enter the VLAN ID used here. This value must be between 1 and 4094.
mask - (Optional) Specifies an additional mask parameter that can be configured.
<hex 0x0-0x0fff> - Enter the mask value here.

source_mac - (Optional) Specifies the source MAC address.
<macaddr> - Enter the source MAC address used for this configuration here.
mask - (Optional) Specifies an additional mask parameter that can be configured.
<macmask> - Enter the source MAC mask used here.

destination_mac - (Optional) Specifies the destination MAC address.
<macaddr> - Enter the destination MAC address used for this configuration here.
mask - (Optional) Specifies an additional mask parameter that can be configured.
<macmask> - Enter the destination MAC mask here.

802.1p - (Optional) Specifies the value of the 802.1p priority tag. The priority tag ranges from 1 to 7.
<value 0-7> - Enter the 802.1p priority tag value here.

ethernet_type - (Optional) Specifies the Ethernet type.
<hex 0x0-0xffff> - Enter the Ethernet type mask here.

ip - (Optional) Specifies to configure the IP access profile.

vlan - (Optional) Specifies a VLAN name.
<vlan_name 32> - Enter the name of the VLAN here. This name can be up to 32 characters long.
vlan_id - (Optional) Specifies that VLAN ID used.
<vlanid 1-4094> - Enter the VLAN ID used here. This value must be between 1 and 4094.
mask - Specifies an additional mask parameter that can be configured.
<hex 0x0-0x0fff> - Enter the mask value here.

source_ip - (Optional) Specifies an IP source address.
<ipaddr> - Enter the source IP address used for this configuration here.
mask - Specifies an additional mask parameter that can be configured.
<netmask> - Enter the source netmask used here.

destination_ip - (Optional) Specifies an IP destination address.
<ipaddr> - Enter the destination IP address used for this configuration here.
mask - Specifies an additional mask parameter that can be configured.
<netmask> - Enter the destination netmask used here.

dscp - (Optional) Specifies the value of DSCP. The DSCP value ranges from 0 to 63.
<value> - Enter the DSCP value here.

icmp - (Optional) Specifies to configure the ICMP parameters.
type - Specifies that the rule will apply to the ICMP Type traffic value.
<value 0-255> - Enter the ICMP type traffic value here. This value must be between 0 and 255.
code - Specifies that the rule will apply to the ICMP Code traffic value.
<value 0-255> - Enter the ICMP code traffic value here. This value must be between 0 and 255.

igmp - (Optional) Specifies to configure the IGMP parameters.
type - Specifies that the rule will apply to the IGMP Type traffic value.
<value 0-255> - Enter the IGMP type traffic value here. This value must be between 0 and 255.

tcp - Specifies to configure the TCP parameters.
src_port - (Optional) Specifies that the rule will apply to a range of TCP source ports.

<value 0-65535> - Enter the TCP source port value here. This value must be between 0 and 65535.

mask - (Optional) Specifies an additional mask parameter that can be configured.

<hex 0x0-0xffff> - Enter the source port mask here.

dst_port - (Optional) Specifies that the rule will apply to a range of TCP destination ports.

<value 0-65535> - Enter the TCP destination port value here. This value must be between 0 and 65535.

mask - (Optional) Specifies an additional mask parameter that can be configured.

<hex 0x0-0xffff> - Enter the destination port mask here.

flag - (Optional) Specifies the TCP flag fields.

all - Specifies that all the TCP flags will be used in this configuration.

urg - Specifies that the TCP flag field will be set to 'urg'.

ack - Specifies that the TCP flag field will be set to 'ack'.

psh - Specifies that the TCP flag field will be set to 'psh'.

rst - Specifies that the TCP flag field will be set to 'rst'.

syn - Specifies that the TCP flag field will be set to 'syn'.

fin - Specifies that the TCP flag field will be set to 'fin'.

udp - Specifies to configure the UDP parameters.

src_port - (Optional) Specifies the UDP source port range.

<value 0-65535> - Enter the UDP source port value here. This value must be between 0 and 65535.

mask - (Optional) Specifies an additional mask parameter that can be configured.

<hex 0x0-0xffff> - Enter the source port mask here,

dst_port - (Optional) Specifies the UDP destination port range.

<value 0-65535> - Enter the UDP destination port value here. This value must be between 0 and 65535.

mask - (Optional) Specifies an additional mask parameter that can be configured.

<hex 0x0-0xffff> - Enter the destination port mask here.

protocol_id - Specifies that the rule will apply to the value of IP protocol ID traffic.

<value 0-255> - Enter the protocol ID used here.

user_define - (Optional) Specifies that the rule will apply to the IP protocol ID and that the mask options behind the IP header , which has a length of 20 bytes.

<hex 0x0-0xffffffff> - Enter the user-defined mask value here.

mask - Specifies an additional mask parameter that can be configured.

<hex 0x0-0xffffffff> - Enter the mask value here.

packet_content - A maximum of 11 offsets can be specified. Each offset defines 2 bytes of data which is identified as a single UDF field. The offset reference is also configurable. It can be defined to start at the end of the tag, the end of the ether type or the end of the IP header. To qualify the fields before the end of the tag, the destination address, source address, and the VLAN tags are also included

offset_chunk_1 – (Optional) Specifies the value of the packet bytes to be matched. Offset chunk 1 will be used.

<hex 0x0-0xffffffff> - Enter the offset chunk 1 mask here.

offset_chunk_2 - (Optional) Specifies the value of the packet bytes to be matched. Offset chunk 2 will be used.

<hex 0x0-0xffffffff> - Enter the offset chunk 2 mask here.

offset_chunk_3 - (Optional) Specifies the value of the packet bytes to be matched. Offset chunk 3 will be used.

<hex 0x0-0xffffffff> - Enter the offset chunk 3 mask here.

offset_chunk_4 - (Optional) Specifies the value of the packet bytes to be matched. Offset chunk 4 will be used.

<hex 0x0-0xffffffff> - Enter the offset chunk 4 mask here.

ipv6 - Specifies that the rule applies to IPv6 fields.

class - (Optional) Specifies the value of the IPv6 class.

<value 0-255> - Enter the IPv6 class value here. This value must be between 0 and 255.

flowlabel - (Optional) Specifies the value of the IPv6 flow label.

<hex 0x0-0xffff> - Enter the IPv6 flow label mask used here.

source_ipv6 - (Optional) Specifies the value of the IPv6 source address.

<ipv6addr> - Enter the source IPv6 address used for this configuration here.

mask - (Optional) Specifies an additional mask parameter that can be configured.
<ipv6mask> - Enter the source IPv6 mask here.

destination_ipv6 - (Optional) Specifies the value of the IPv6 destination address.
<ipv6addr> - Enter the destination IPv6 address used for this configuration here.
mask - (Optional) Specifies an additional mask parameter that can be configured.
<ipv6mask> - Enter the destination IPv6 mask here.

tcp - (Optional) Specifies to configure the TCP parameters.
src_port - Specifies the value of the IPv6 Layer 4 TCP source port.
<value 0-65535> - Enter the TCP source port value here. This value must be between 0 and 65535.
mask - Specifies an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the TCP source port mask value here.
dst_port - (Optional) Specifies the value of the IPv6 Layer 4 TCP destination port.
<value 0-65535> - Enter the TCP destination port value here. This value must be between 0 and 65535.
mask - Specifies an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the TCP destination port mask value here.

udp - (Optional) Specifies to configure the UDP parameters.
src_port - Specifies the value of the IPv6 Layer 4 UDP source port.
<value 0-65535> - Enter the UDP source port value here. This value must be between 0 and 65535.
mask - Specifies an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the UDP source port mask value here.
dst_port - Specifies the value of the IPv6 Layer 4 UDP destination port.
<value 0-65535> - Enter the UDP destination port value here. This value must be between 0 and 65535.
mask - Specifies an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the UDP destination port mask value here.

icmp - (Optional) Specifies to configure the ICMP parameters used.
type - Specifies that the rule applies to the value of ICMP type traffic.
<value 0-255> - Enter the ICMP type traffic value here. This value must be between 0 and 255.
code - Specifies that the rule applies to the value of ICMP code traffic.
<value 0-255> - Enter the ICMP code traffic value here. This value must be between 0 and 255.

port - Specifies the port list used for this configuration.
<portlist> - Enter a list of ports used for the configuration here.
all - Specifies that all the ports will be used for this configuration.

vlan_based - Specifies that the rule will be VLAN based.
vlan - Specifies the VLAN name used for this configuration.
<vlan_name> - Enter the VLAN name used for this configuration here.
vlan_id - Specifies the VLAN ID used for this configuration.
<vlanid 1-4094> - Enter the VLAN ID used here. This value must be between 1 and 4094.

permit - Specifies that packets matching the access rule are permitted by the Switch.

priority - (Optional) Specifies that the priority of the packet will change if the packet matches the access rule.
<value 0-7> - Enter the priority value here. This value must be between 0 and 7.

replace_priority - (Optional) Specifies that the 802.1p priority of the outgoing packet will be replaced.
replace_dscp_with - (Optional) Specifies that the DSCP of the outgoing packet is changed with the new value. If using this action without an action priority, the packet will be sent to the default TC.
<value 0-63> - Enter the replace DSCP with value here. This value must be between 0 and 63.
replace_tos_precedence_with - (Optional) Specifies that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC.
<value 0-7> - Enter the replace ToS precedence with value here. This value must be between 0 and 7.

counter - (Optional) Specifies whether the ACL counter feature is enabled or disabled. This parameter is optional. The default option is disabled. If the rule is not bound with the flow_meter, all matching packets are counted. If the rule is bound with the flow_meter, then the “counter” is overridden.

enable - Specifies that the ACL counter feature will be enabled.

disable - Specifies that the ACL counter feature will be disabled.

deny - Specifies that packets matching the access rule are filtered by the Switch.

mirror - Specifies that packets matching the access rules are copied to the mirror port.

time_range - (Optional) Specifies the name of the time range entry.

<range_name 32> - Enter the time range name here. This name can be up to 32 characters long.

delete - Specifies that a profile or a rule will be deleted.

access_id - Specifies the index of the access list entry. The value range is 1-256, but the supported maximum number of entries depends on the project. If the auto_assign option is selected, the access ID is automatically assigned, when adding multiple ports.

<value 1-256> - Enter the access ID used here. This value must be between 1 and 256.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a rule entry for a packet content mask profile (option 3):

```
DWS-3160-24PC:admin#config access_profile profile_id 4 add access_id
auto_assign packet_content offset_chunk_1 0xFFFFFFFF port all deny
Command: config access_profile profile_id 4 add access_id auto_assign
packet_content offset_chunk_1 0xFFFFFFFF port all deny


Success.


DWS-3160-24PC:admin#
```

6-4 show access_profile

Description

This command is used to display an access profile including current access list entries.

Format

show access_profile {[profile_id <value 1-6> | profile_name <name 1-32>]}

Parameters

profile_id - (Optional) Specifies the index of the access list profile.

<value 1-6> - Enter the profile ID used here. This value must be between 1 and 6.

profile_name - (Optional) Specifies the name of the profile.

<name 1-32> - Enter the profile name used here. This name can be up to 32 characters long.

Restrictions

None.

Example

To display the current access list table:

```
DWS-3160-24PC:admin#show access_profile
Command: show access_profile

Access Profile Table

Total User Set Rule Entries : 1
Total Used HW Entries       : 1
Total Available HW Entries  : 1535

===============================================================================
Profile ID: 1     Profile name: t1  Type: Ethernet

MASK on
    VLAN            : 0xFFF
    Source MAC      : 00-00-00-00-00-01
    Destination MAC : 00-00-00-00-00-02
    802.1p
    Ethernet Type

Available HW Entries : 256
===============================================================================

===============================================================================
Profile ID: 2     Profile name: 2  Type: IPv4

MASK on
    VLAN            : 0xFFF
    Source IP       : 20.0.0.0
    Dest IP         : 10.0.0.0
    DSCP
    ICMP
    Type
    Code

Available HW Entries : 256
===============================================================================

===============================================================================
Profile ID: 4     Profile name: 4  Type: User Defined

MASK on
    offset_chunk_1 : 3      value : 0x0000FFFF
    offset_chunk_2 : 5      value : 0x0000FF00
    offset_chunk_3 : 14     value : 0xFFFF0000
    offset_chunk_4 : 16     value : 0xFF000000

Available HW Entries : 255
-------------------------------------------------------------------------------
```

```
Rule ID : 1    (auto assign)    Ports: 1-24

Match on
    offset_chunk_1 : 3      value : 0x0000FFFF

Action:
    Deny

===============================================================================

DWS-3160-24PC:admin#
```

The following example displays an access profile that supports an entry mask for each rule:

```
DWS-3160-24PC:admin#show access_profile profile_id 2
Command: show access_profile profile_id 2

Access Profile Table

===============================================================================
Profile ID: 2     Profile name: 2  Type: IPv4

MASK on
    VLAN            : 0xFFF
    Source IP       : 20.0.0.0
    Dest IP         : 10.0.0.0
    DSCP
    ICMP
    Type
    Code

Available HW Entries : 256
===============================================================================

DWS-3160-24PC:admin#
```

The following example displays the packet content mask profile for the profile with an ID of 4:

```
DWS-3160-24PC:admin#show access_profile profile_id 4
Command: show access_profile profile_id 4

Access Profile Table

===============================================================================
Profile ID: 4     Profile name: 4  Type: User Defined

MASK on
    offset_chunk_1 : 3      value : 0x0000FFFF
    offset_chunk_2 : 5      value : 0x0000FF00
    offset_chunk_3 : 14     value : 0xFFFF0000
    offset_chunk_4 : 16     value : 0xFF000000

Available HW Entries : 255
-------------------------------------------------------------------------------
Rule ID : 1    (auto assign)    Ports: 1-24

Match on
    offset_chunk_1 : 3      value : 0x0000FFFF

Action:
    Deny

===============================================================================

DWS-3160-24PC:admin#
```

6-5 config flow_meter

Description

This command is used to configure the flow-based metering function. The metering function supports three modes: single rate two color, single rate three color, and two rate three color. The access rule must be created before the parameters of this function can be applied.

For the single rate two color mode, users may set the preferred bandwidth for this rule, in Kbps, and once the bandwidth has been exceeded, overflowing packets will either be dropped or have a drop precedence set, depending on the user configuration.

For single rate three color mode, users need to Specifies the committed rate, in Kbps, the committed burst size, and the excess burst size.

For the two rate three color mode, users need to Specifies the committed rate in Kbps, the committed burst size, the peak rate and the peak burst size.

There are two cases for mapping the color of a packet: Color-blind mode and Color-aware mode. In the Color-blind case, the determination for the packet’s color is based on the metering result. In the Color-aware case, the determination for the packet’s color is based on the metering result and the ingress DSCP.

When color-blind or color-aware is not specified, color-blind is the default mode.

The green color packet will be treated as the conforming action, the yellow color packet will be treated as the exceeding action, and the red color packet will be treated as the violating action.

The replace DSCP action can be performed on packets that conform (GREEN) and packets that do not conform (YELLOW and RED). If drop YELLOW/RED is selected, the action to replace the DSCP will not take effect.

Format

config flow_meter [profile_id <value 1-6> | profile_name <name 1-32>] access_id <value 1-256> [rate [<value 0-1048576>] {burst_size [<value 0-131072>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 0-1048576> {cbs <value 0-131072>} pir <value 0-1048576> {pbs <value 0-131072>} {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | sr_tcm cir <value 0-1048576> cbs <value 0-131072> ebs <value 0-131072> {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | delete]

Parameters

profile_id - Specifies the profile ID.
<value 1-6> - Enter the profile ID here. This value must be between 1 and 6.

profile_name - Specifies the name of the profile. The maximum length is 32 characters.
<name 1-32> - Enter the profile name used here.

access_id - Specifies the access ID.
<value 1-256> - Enter the access ID used here. This value must be between 1 and 256.

rate - This specifies the rate for single rate two color mode. Specifies the committed bandwidth in Kbps for the flow.
<value 0-1048576> - Enter the rate for single rate two color mode here. This value must be between 0 and 1048576.

burst_size - (Optional) This specifies the burst size for the single rate two color mode. The unit is Kbytes.
<value 0-131072> - Enter the burst size value here. This value must be between 0 and 131072.

rate_exceed - This specifies the action for packets that exceeds the committed rate in single rate, two color mode.
drop_packet - Drop the packet immediately.
remark_dscp - Mark the packet with a specified DSCP. The packet is set to have a high drop precedence.
<value 0-63> - Enter the remark DSCP value here. This value must be between 0 and 63.

tr_tcm - Specifies the “two rate three color mode”.

cir - Specifies the “Committed Information Rate”. The unit is in Kbps. CIR should always be equal or less than PIR.
<value 0-1048576> - Enter the committed information rate value here. This value must be between 0 and 1048576.

cbs - (Optional) Specifies the “Committed Burst Size”. The unit is Kbytes. That is to say, 1 means 1Kbytes. This parameter is an optional parameter. The default value is 4*1024.
<value 0-1048576> - Enter the committed burst size value here. This value must be between 0 and 1048576.

pir - Specifies the “Peak Information Rate”. The unit is in Kbps. PIR should always be equal to or greater than CIR.
<value 0-1048576> - Enter the peak information rate value here. This value must be between 0 and 1048576.

pbs - (Optional) Specifies the “Peak Burst Size”. The unit is in Kbytes. This parameter is an optional parameter. The default value is 4*1024.
<value 0-131072> - Enter the peak burst size value here. This value must be between 0 and

131072.

color_blind - (Optional) Specifies the meter mode as color-blind. The default is color-blind mode.
color_aware - (Optional) Specifies the meter mode as color-aware. The final color of the packet is determined by the initial color of the packet and the metering result.

conform - (Optional) Specifies the action when a packet is mapped to the “green” color.
permit - Permits the packet.
replace_dscp - Changes the DSCP of the packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.

counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
enable - Specifies that the ACL counter option will be enabled.
disable - Specifies that the ACL counter option will be disabled.

replace_dscp - (Optional) Changes the DSCP of an un-conforming (yellow or red) packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.

exceed - Specifies the action when a packet is mapped to the “yellow” color.
permit - Permits the packet.
replace_dscp - Changes the DSCP of the packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.
drop - Drops the packet.

counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
enable - Specifies that the ACL counter option will be enabled.
disable - Specifies that the ACL counter option will be disabled.

violate - Specifies the action when a packet is mapped to the “red” color.
permit - Permits the packet.
replace_dscp - Changes the DSCP of the packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.
drop - Drops the packet.

counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
enable - Specifies that the ACL counter option will be enabled.
disable - Specifies that the ACL counter option will be disabled.

sr_tcm - Specifies “single rate three color mode”.

cir - Specifies the “Committed Information Rate”. The unit is Kbps.
<value 0-1048576> - Enter the committed information rate value here. This value must be between 0 and 1048576.

cbs - Specifies the “Committed Burst Size” The unit is Kbytes.
<value 0-131072> - Enter the committed burst size value here. This value must be between 0 and 131072.

ebs - Specifies the “Excess Burst Size”. The unit is Kbytes.
<value 0-131072> - Enter the excess burst size value here. This value must be between 0 and 131072.

color_blind - (Optional) Specifies the meter mode as color-blind. The default is color-blind mode.
color_aware - (Optional) Specifies the meter mode as color-aware. The final color of the packet is determined by the initial color of the packet and the metering result.

conform - (Optional) Specifies the action when a packet is mapped to the “green” color.
permit - Permits the packet.
replace_dscp - Changes the DSCP of the packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.

counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
enable - Specifies that the ACL counter option will be enabled.
disable - Specifies that the ACL counter option will be disabled.

exceed - Specifies the action when a packet is mapped to the “yellow” color.
permit - Permits the packet.

replace_dscp - Changes the DSCP of the packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.
drop - Drops the packet.

counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
enable - Specifies that the ACL counter option will be enabled.
disable - Specifies that the ACL counter option will be disabled.

violate - Specifies the action when a packet is mapped to the “red” color.
permit - Permits the packet.
replace_dscp - Changes the DSCP of the packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.
drop - Drops the packet.

counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
enable - Specifies that the ACL counter option will be enabled.
disable - Specifies that the ACL counter option will be disabled.

delete - Deletes the specified flow_meter.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a “two rate, three color” flow meter:

```
DWS-3160-24PC:admin#config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000
cbs 2000 pir 2000 pbs 2000 color_blind conform permit counter enable exceed
permit replace_dscp 60 counter enable violate drop
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 2000
pir 2000 pbs 2000 color_blind conform permit counter enable exceed permit
replace_dscp 60 counter enable violate drop


Success.
DWS-3160-24PC:admin#
```

6-6 show flow_meter

Description

This command is used to display the flow-based metering (ACL Flow Metering) configuration.

Format

show flow_meter {[profile_id <value 1-6> | profile_name <name 1-32>] {access_id <value 1-256>}}

Parameters

profile_id - (Optional) Specifies the profile ID.
<value 1-6> - Enter the profile ID used here. This value must be between 1 and 6.

profile_name - (Optional) Specifies the name of the profile. The maximum length is 32 characters.
<name 1-32> - Enter the profile name used here.

access_id - (Optional) Specifies the access ID.
<value 1-256> - Enter the access ID used here. This value must be between 1 and 256.

Restrictions

None.

Example

To display the flow metering configuration:

```
DWS-3160-24PC:admin#show flow_meter
Command: show flow_meter

Flow Meter Information
------------------------------------------------------------------------------
Profile ID:1     Aceess ID:1     Mode : trTCM / ColorBlind
CIR(Kbps):1000     CBS(Kbyte):2000     PIR(Kbps):2000     PBS(Kbyte):2000
Action:
      Conform : Permit                        Counter: Enabled
       Exceed : Permit     Replace DSCP: 60   Counter: Enabled
      Violate : Drop                          Counter: Disabled
------------------------------------------------------------------------------

Total Entries: 1

DWS-3160-24PC:admin#
```

6-7 config time_range

Description

This command is used to define a specific range of time to activate a function on the Switch by specifying which time range in a day and which days in a week are covered in the time range.

NOTE: The specified time range is based on the SNTP time or the configured time. If this time is not available, the time range will not be met.

Format

config time_range <range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> | delete]

Parameters

time_range - Specifies the name of the time range settings.
<range_name 32> - Enter the time range name used here. This name can be up to 32 characters long.

hours - Specifies the time of a day.
start_time - Specifies the starting time of a day.
<time hh:mm:ss> - Enter the starting time here. (24-hr time). For example, 19:00 means 7PM. 19 is also acceptable. The time specified in the start_time parameter must be smaller than the time specified in the end_time parameter.

end_time - Specifies the ending time of a day. (24-hr time)
<time hh:mm:ss> - Enter the ending time here. (24-hr time). For example, 19:00 means 7PM. 19 is also acceptable. The time specified in the start_time parameter must be smaller than the time specified in the end_time parameter.

weekdays - Specifies the list of days contained in the time range. Use a dash to define a period of days. Use a comma to separate specific days.
<daylist> - Enter the weekdays that will be included in this configuration here. For example, mon-fri (Monday to Friday). sun, mon, fri (Sunday, Monday and Friday)

delete - Deletes a time range profile. When a time_range profile has been associated with ACL entries, deleting the time_range profile will fail.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a time range named “1” that starts every Monday at 01:01:01am and ends at 02:02:02am:

```
DWS-3160-24PC:admin# config time_range 1 hours start_time 1:1:1 end_time 2:2:2
weekdays mon
Command: config time_range 1 hours start_time 1:1:1 end_time 2:2:2 weekdays mon

Success.

DWS-3160-24PC:admin# config time_range 1 delete
Command: config time_range 1 delete

Success.

DWS-3160-24PC:admin#
```

6-8 show time_range

Description

This command is used to display the current time range settings.

Format

show time_range

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To display the current time range settings:

```
DWS-3160-24PC:admin#show time_range
Command: show time_range

Time Range Information
-------------------------
Range Name   :  1
Weekdays     :  Mon
Start Time   :  01:01:01
End Time     :  02:02:02

Total Entries :1

DWS-3160-24PC:admin#
```

6-9 show current_config access_profile

Description

This command is used to display the ACL part of the current configuration, when logged in with user level privileges.

The overall current configuration can be displayed by using the show config command, which is accessible with administrator level privileges.

Format

show current_config access_profile

Parameters

None.

Restrictions

None.

Example

To display the ACL part of the current configuration:

```
DWS-3160-24PC:admin#show current_config access_profile
Command: show current_config access_profile
#------------------------------------------------------------------------------

# ACL

create access_profile profile_id 1 profile_name t1 ethernet vlan 0xFFF
source_mac 00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p
ethernet_type
config access_profile profile_id 1 add access_id 1 ethernet vlan_id 2
source_mac 00-11-22-33-44-55 destination_mac 00-12-34-56-78-90 802.1p 1
ethernet_type 0xFFFF port 10 permit priority 1 replace_priority replace_tos 1
counter enable time_range 1
create access_profile profile_id 2 profile_name 2 ip vlan source_ip_mask
20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type code
create access_profile profile_id 4 profile_name 4 packet_content_mask
offset_chunk_1 3 0xFFFF offset_chunk_2 5 0xFF00 offset_chunk_3 14 0xFFFF0000
offset_chunk_4 16 0xFF000000
config access_profile profile_id 4 add access_id auto_assign packet_content
offset_chunk_1 0xFFFFFFFF port 1-24 deny

#------------------------------------------------------------------------------

DWS-3160-24PC:admin#
```

Chapter 7 Access Control List (ACL) Egress Command List

create egress_access_profile profile_id <value 1-4> profile_name <name 1-32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask<hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | ipv6 {class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}]

delete egress_access_profile [profile_id <value 1-4> | profile_name <name 1-32> | all]

config egress_access_profile [profile_id <value 1-4> | profile_name <name 1-32>] [add access_id [auto_assign | <value 1-128>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp<value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]} | ipv6 {class <value 0-255> | source_ipv6 <ipv6addr> {mask <ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type <value 0-255> | code <value 0-255>}]}] [vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] | port_group [id <value 1-64> | name <name 16>] | port <port>] [permit {replace_priority_with <value 0-7> | replace_dscp_with <value 0-63> | counter [enable | disable]} | deny] {time_range <range_name 32>} | delete access_id <value 1-128>]

show egress_access_profile {[profile_id <value 1-4> | profile_name <name 1-32>]}

show current_config egress_access_profile

config egress_flow_meter [profile_id <value 1-4> | profile_name <name 1-32>] access_id <value 1-128> [rate [<value>] {burst_size [<value>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value> {cbs <value>} pir <value> {pbs <value>} {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | sr_tcm cir <value> cbs <value> ebs <value> {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | delete]

show egress_flow_meter {[profile_id <value 1-4> | profile_name <name 1-32>] {access_id <value 1-128>}}

create port_group id <value 1-64> name <name 16>

config port_group [id <value 1-64> | name <name 16>] [add | delete] [<portlist> | all]

delete port_group [id <value 1-64> | name <name 16>]

show port_group {id<value 1-64> | name<name 16>}

7-1 create egress_access_profile

Description

This command is used to create an egress access list profile. For example, for some hardware, it may be invalid to Specifies destination IPv6 address and source IPv6 address at the same time. The user will be prompted for these limitations.

Format

create egress_access_profile profile_id <value 1-4> profile_name <name 1-32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | ipv6 {class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}]

Parameters

profile_id - Specifies the index of the egress access list profile.
<value 1-4> - Enter the profile ID used here. This value must be between 1 and 4.

profile_name - The name of the profile must be specified. The maximum length is 32 characters.
<name 1-32> - Enter the profile name used here. This name can be up to 32 characters long.

ethernet - Specifies this is an Ethernet mask.

vlan - (Optional) Specifies a VLAN mask.
<hex 0x0-0x0fff> - Enter the VLAN mask used here.

source_mac - (Optional) Specifies the source MAC mask.
<macmask> - Enter the source MAC mask used here.

destination_mac - (Optional) Specifies the destination MAC mask.
<macmask> - Enter the destination MAC mask used here.

802.1p - (Optional) Specifies 802.1p priority tag mask.

ethernet_type - (Optional) Specifies the Ethernet type mask.

ip - Specifies this is an IPv4 mask.

vlan - (Optional) Specifies a VLAN mask.
<hex 0x0-0x0fff> - Enter the VLAN mask used here.

source_ip_mask - (Optional) Specifies a source IP address mask.
<netmask> - Enter the source network mask used here.

destination_ip_mask - (Optional) Specifies a destination IP address mask.
<netmask> - Enter the destination network mask used here.

dscp - (Optional) Specifies the DSCP mask.

icmp - (Optional) Specifies that the rule applies to ICMP traffic.
type - Specifies the type of ICMP traffic.
code - Specifies the code of ICMP traffic.

igmp - (Optional) Specifies that the rule applies to IGMP traffic.
type - Specifies the type of IGMP traffic.

tcp - (Optional) Specifies that the rule applies to TCP traffic.
src_port_mask - Specifies the TCP source port mask.
<hex 0x0-0xffff> - Enter the TCP source port mask value here.
dst_port_mask - Specifies the TCP destination port mask.
<hex 0x0-0xffff> - Enter the TCP source port mask value here.

flag_mask - (Optional) Specifies the TCP flag field mask.

all - Specifies that the TCP flag field mask will be set to 'all'.
urg - Specifies that the TCP flag field mask will be set to 'urg'.
ack - Specifies that the TCP flag field mask will be set to 'ack'.
psh - Specifies that the TCP flag field mask will be set to 'psh'.
rst - Specifies that the TCP flag field mask will be set to 'rst'.
syn - Specifies that the TCP flag field mask will be set to 'syn'.
fin - Specifies that the TCP flag field mask will be set to 'fin'.

udp - (Optional) Specifies that the rule applies to UDP traffic.
src_port_mask - Specifies the UDP source port mask.
<hex 0x0-0xffff> - Enter the UDP source port mask value here.
dst_port_mask - Specifies the UDP destination port mask.
<hex 0x0-0xffff> - Enter the UDP destination port mask value here.

protocod_id_mask - (Optional) Specifies that the rule applies to IP protocol ID traffic.
<hex 0x0-0xff> - Enter the protocol ID mask value here.

user_define_mask - (Optional) Specifies that the rule applies to the IP protocol ID, and that the mask option behind the IP header length is 20 bytes.
<hex 0x0-0xffffffff> - Enter the user-defined mask value here.

ipv6 - (Optional) Specifies this is an IPv6 mask.

class - (Optional) Specifies the IPv6 class.

source_ipv6_mask - (Optional) Specifies an IPv6 source sub-mask.
<ipv6mask> - Enter the IPv6 source sub-mask value here.
destination_ipv6_mask - Specifies an IPv6 destination sub-mask.
<ipv6mask> - Enter the IPv6 destination sub-mask value here.

tcp - (Optional) Specifies that the following parameter are application to the TCP configuration.
src_port_mask - Specifies an IPv6 Layer 4 TCP source port mask.
<hex 0x0-0xffff> - Enter the Ipv6 TCP source port mask value here.
dst_port_mask - Specifies an IPv6 Layer 4 TCP destination port mask.
<hex 0x0-0xffff> - Enter the Ipv6 TCP destination port mask value here.

udp - (Optional) Specifies that the following parameter are application to the UDP configuration.
src_port_mask - Specifies an IPv6 Layer 4 UDP source port mask.
<hex 0x0-0xffff> - Enter the Ipv6 UDP source port mask value here.
dst_port_mask - Specifies an IPv6 Layer 4 UDP destination port mask.
<hex 0x0-0xffff> - Enter the Ipv6 UDP destination port mask value here.

icmp - (Optional) Specifies that the rule applies to ICMP traffic.
type - Specifies the type of ICMP traffic.
code - Specifies the code of ICMP traffic.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an egress access list profile with the name “eap-eth-bc” and assign the profile ID to be 1:

```
DWS-3160-24PC:admin# create egress_access_profile profile_id 1 profile_name
eap-eth-bc ethernet source_mac FF-FF-FF-FF-FF-FF
Command: create egress_access_profile profile_id 1 profile_name eap-eth-bc
ethernet source_mac FF-FF-FF-FF-FF-FF


DWS-3160-24PC:admin#
```

7-2 delete egress_access_profile

Description

This command is used to delete an egress access profile.

Format

delete egress_access_profile [profile_id <value 1-4> | profile_name <name 1-32> | all]

Parameters

profile_id - Specifies the index of the egress access list profile.
<value 1-4> - Enter the profile ID used here. This value must be between 1 and 4.

profile_name - Specifies the name of the profile. The maximum length is 32 characters.
<name 1-32> - Enter the profile name used here. This name can be up to 32 characters long.

all - Specifies that the whole egress access list profile will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete egress access list profile ID 1:

```
DWS-3160-24PC:admin# delete egress_access_profile profile_id 1
Command: delete egress_access_profile profile_id 1

Success.

DWS-3160-24PC:admin#
```

7-3 config egress_access_profile

Description

This command is used to configure egress access list entries.

Format

config egress_access_profile [profile_id <value 1-4> | profile_name <name 1-32>] [add access_id [auto_assign | <value 1-128>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]} | ipv6 {class <value 0-255> | source_ipv6 <ipv6addr> {mask <ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type <value 0-255> | code <value 0-255>}]}] [vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] | port_group [id <value 1-64> | name <name 16>] | port <port>] [permit {replace_priority_with

<value 0-7> | replace_dscp_with <value 0-63> | counter [enable | disable]} | deny] {time_range <range_name 32>} | delete access_id <value 1-128>]

Parameters

profile_id - Specifies the index of the egress access list profile.
<value 1-4> - Enter the profile ID used here. This value must be between 1 and 4.

profile_name - Specifies the name of the profile.
<name 1-32> - Enter the profile name here. This name can be up to 32 characters long.

add - Specifies to add a profile or rule.

access_id - Specifies the index of the access list entry. If the auto_assign option is selected, the access ID is automatically assigned.
auto assign - Specifies that the access ID will be configured automatically.
<value 1-128> - Enter the access ID used here. This value must be between 1 and 128.

ethernet - Specifies an Ethernet egress ACL rule.

vlan - (Optional) Specifies the VLAN name.
<vlan_name 32> - Enter the VLAN name used for this configuration here. This name can be up to 32 characters long.
vlanid - Specifies a VLAN ID.
<vlanid 1-4094> - Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.

source_mac - (Optional) Specifies the source MAC address.
<macaddr> - Enter the source MAC address used here.
mask - Specifies that source MAC mask used.
<macmask> - Enter the source MAC mask value here.
destination_mac - Specifies the destination MAC address.
<macaddr> - Enter the destination MAC address used here.
mask - Specifies that destination MAC mask used.
<macmask> - Enter the destination MAC mask value here.

802.1p - (Optional) Specifies the value of the 802.1p priority tag. The priority tag ranges from 1 to 7.
<value 0-7> - Enter the 802.1p priority tag used here.

ethernet_type - (Optional) Specifies the Ethernet type.
<hex 0x0-0xffff> - Enter the Ethernet type mask used here.

ip - Specifies an IP egress ACL rule.

vlan - (Optional) Specifies the VLAN name.
<vlan_name 32> - Enter the VLAN name used for this configuration here. This name can be up to 32 characters long.
vlanid - Specifies a VLAN ID.
<vlanid 1-4094> - Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.

mask - (Optional) Specifies the mask used.
<hex 0x0-x0fff> - Enter the mask value used here.

source_ip - (Optional) Specifies an IP source address.
<ipaddr> - Enter the source IP address used here.
mask - Specifies the source IP address used here.
<netmask> - Enter the source network mask here.

destination_ip - (Optional) Specifies an IP destination address.
<ipaddr> - Enter the destination IP address used here.
mask - Specifies the destination IP address used here.
<netmask> - Enter the destination network mask here.

dscp - (Optional) Specifies the value of DSCP. The DSCP value ranges from 0 to 63.
<value 0-63> - Enter the DSCP value used here. This value must be between 0 and 63.

icmp - (Optional) Specifies that the following parameters configured will apply to the ICMP configuration.
type - Specifies that the rule will apply to the ICMP type traffic value.
<value 0-255> - Enter the ICMP traffic type value here. This value must be between 0 and 255.

code - Specifies that the rule will apply to the ICMP code traffic value.
<value 0-255> - Enter the ICMP code traffic value here. This value must be between 0 and 255.

igmp - (Optional) Specifies that the following parameters configured will apply to the IGMP configuration.
type - Specifies that the rule will apply to the IGMP type traffic value.
<value 0-255> - Enter the IGMP type traffic value here. This value must be between 0 and 255.

tcp - (Optional) Specifies that the following parameters configured will apply to the TCP configuration.
src_port - Specifies that the rule will apply to a range of TCP source ports.
<value 0-65535> - Enter the source port value here. This value must be between 0 and 65535.
mask - Specifies the TCP source port mask here.
<hex 0x0-0xffff> - Enter the TCP source port mask value here.
dst_port - Specifies that the rule will apply to a range of TCP destination ports.
<value 0-65535> - Enter the destination port value here. This value must be between 0 and 65535.
mask - Specifies the TCP destination port mask here.
<hex 0x0-0xffff> - Enter the TCP destination port mask value here.

flag - (Optional) Specifies the TCP flag fields.
all - Specifies that the TCP flag field will be set to 'all'.
urg - Specifies that the TCP flag field will be set to 'urg'.
ack - Specifies that the TCP flag field will be set to 'ack'.
psh - Specifies that the TCP flag field will be set to 'psh'.
rst - Specifies that the TCP flag field will be set to 'rst'.
syn - Specifies that the TCP flag field will be set to 'syn'.
fin - Specifies that the TCP flag field will be set to 'fin'.

udp - (Optional) Specifies that the following parameters configured will apply to the UDP configuration.
src_port - Specifies the UDP source port range.
<value 0-65535> - Enter the UDP source port range value here.
mask - Specifies the UDP source port mask here.
<hex 0x0-0xffff> - Enter the UDP source port mask value here.
dst_port - Specifies the UDP destination port range.
<value 0-65535> - Enter the UDP destination port range value here.
mask - Specifies the UDP destination port mask here.
<hex 0x0-0xffff> - Enter the UDP destination port mask value here.

protocol_id - (Optional) Specifies that the rule will apply to the value of IP protocol ID traffic.
<value 0-255> - Enter the protocol ID used here. This value must be between 0 and 255.

user_define - (Optional) Specifies that the rule will apply to the IP protocol ID and that the mask options behind the IP header, which has a length of 20 bytes.
<hex 0x0-0xffffffff> - Enter the user-defined mask value here.
mask - Specifies the user-defined mask here.
<hex 0x0-0xffffffff> - Enter the user-defined mask value here.

ipv6 - Specifies the rule applies to IPv6 fields.

class - (Optional) Specifies the value of IPv6 class.
<value 0-255> - Enter the IPv6 class value here. This value must be between 0 and 255.

source_ipv6 - (Optional) Specifies the value of IPv6 source address.
<ipv6addr> - Enter the source IPv6 source address here.
mask - Specifies the IPv6 source address mask here.
<ipv6mask> - Enter the IPv6 source address mask value here.

destination_ipv6 - (Optional) Specifies the value of IPv6 destination address.
<ipv6addr> - Enter the source IPv6 destination address here.
mask - Specifies the IPv6 destination address mask here.
<ipv6mask> - Enter the IPv6 destination address mask value here.

tcp - (Optional) Specifies the TCP protocol
src_port - Specifies the value of the IPv6 layer 4 TCP source port.
<value 0-65535> - Enter the IPv6 TCP source port value here. This value must be

between 0 and 65535.
mask - Specifies the IPv6 TCP source port mask here.
<hex 0x0-0xffff> - Enter the IPv6 TCP source port mask value here.
dst_port - Specifies the value of the IPv6 layer 4 TCP destination port.
<value 0-65535> - Enter the IPv6 TCP destination port value here. This value must be between 0 and 65535.
mask - Specifies the IPv6 TCP destination port mask here.
<hex 0x0-0xffff> - Enter the IPv6 TCP destination port mask value here.

udp - (Optional) Specifies the UDP protocol.
src_port - Specifies the value of the IPv6 layer 4 UDP source port.
<value 0-65535> - Enter the IPv6 UDP source port value here. This value must be between 0 and 65535.
mask - Specifies the IPv6 UDP source port mask here.
<hex 0x0-0xffff> - Enter the IPv6 UDP source port mask value here.
dst_port - Specifies the value of the IPv6 layer 4 UDP destination port.
<value 0-65535> - Enter the IPv6 UDP destination port value here. This value must be between 0 and 65535.
mask - Specifies the IPv6 UDP destination port mask here.
<hex 0x0-0xffff> - Enter the IPv6 UDP destination port mask value here.

icmp - (Optional) Specifies that the following parameters configured will apply to the ICMP configuration.
type - Specifies that the rule will apply to the ICMP type traffic value.
<value 0-255> - Enter the ICMP traffic type value here. This value must be between 0 and 255.
code - Specifies that the rule will apply to the ICMP code traffic value.
<value 0-255> - Enter the ICMP code traffic value here. This value must be between 0 and 255.

vlan_based - The rule applies on the specified VLAN.

vlan - Specifies the VLAN name.
<vlan_name 32> - Enter the VLAN name used for this configuration here. This name can be up to 32 characters long.
vlanid - Specifies a VLAN ID.
<vlanid 1-4094> - Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.

port_group - Specifies the port group value here.
id - Specifies the ID of the port group which the rule applies.
<value 1-64> - Enter the group ID value here. This value must be between 1 and 64.
name - Specifies the name of the port group which the rule applies.
<name_string 16> - Enter the port group name here. This name can be up to 16 characters long.

permit - Specifies that packets matching the egress access rule are permitted by the Switch.

replace_priority_with - (Optional) Specifies the packets that match the egress access rule are changed the 802.1p priority tag field by the Switch.
<value 0-7> - Enter the replace priority with value here. This value must be between 0 and 7.
replace_dscp_with - (Optional) Specifies the packets that match the egress access rule are changed the DSCP value by the Switch.
<value 0-63> - Enter the replace DSCP with value here. This value must be between 0 and 63.

counter - (Optional) Specifies whether the ACL counter feature is enabled or disabled. This parameter is optional. The default option is disabled. If the rule is not bound with the flow_meter, all matching packets are counted. If the rule is bound with the flow_meter, then the "counter" is overridden.
enable - Specifies that the ACL counter feature will be enabled.
disable - Specifies that the ACL counter feature will be disabled.

deny - Specifies the packets that match the egress access rule are filtered by the Switch.

time_range - (Optional) Specifies the name of the time range entry.
<range_name 32> - Enter the time range value here. This name can be up to 32 characters long.

delete - Specifies to delete a profile or rule.

access_id - Specifies the index of the access list entry. If the auto_assign option is selected, the access ID is automatically assigned.
<value 1-128> - Enter the access ID used here. This value must be between 1 and 128.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a port-base egress access rule that when the packet go out Switch which match the specified source IP, DSCP and destination IP field, it will not be dropped:

```
DWS-3160-24PC:admin# config egress_access_profile profile_id 2 add access_id
auto_assign ip source_ip 10.0.0.1 dscp 25 destination_ip 10.90.90.90 port_group
id 1 permit
Command: config egress_access_profile profile_id 2 add access_id auto_assign ip
source_ip 10.0.0.1 dscp 25 destination_ip 10.90.90.90 port_group id 1 permit


Success.


DWS-3160-24PC:admin#
```

To configure a vlan-base egress access rule that when the packet go out Switch which match the specified source MAC field, it will be dropped:

```
DWS-3160-24PC:admin# config egress_access_profile profile_id 2 add access_id 1
ethernet source_mac 11-22-33-44-55-66 vlan_based vlan_id 1 deny
Command: config egress_access_profile profile_id 2 add access_id 1 ethernet
source_mac 11-22-33-44-55-66 vlan_based vlan_id 1 deny


Success.


DWS-3160-24PC:admin#
```

7-4 show egress_access_profile

Description

This command is used to display current egress access list table.

Format

show egress_access_profile {[profile_id <value 1-4> | profile_name <name 1-32>]}

Parameters

profile_id - (Optional) Specifies the index of the egress access list profile.
<value 1-4> - Enter the profile ID here. This value must be between 1 and 4.

profile_name - (Optional) Specifies the name of the profile. The maximum length is 32 characters.
<name 1-32> - Enter the profile name here. This name can be up to 32 characters long.

If no parameter is specified, will display the all egress access profile.

Restrictions

None.

Example

To display current egress access list table:

```
DWS-3160-24PC:admin# show egress_access_profile
Command: show access_profile

Egress Access Profile Table

Total User Set Rule Entries       : 3
Total Used Hardware Entries       : 3
Total Available Hardware Entries  : 509

==============================================================================
Profile ID: 1     Profile name: 1  Type: Ethernet

Mask on
    Source MAC      : FF-FF-FF-FF-FF-FF

Available Hardware Entries : 127
------------------------------------------------------------------------------
Rule ID : 1       Port group: -

Match on
    VLAN ID         : 1
    Source MAC      : 00-00-00-00-00-01

Action:
    Permit

==============================================================================

==============================================================================
Profile ID: 2     Profile name: 2  Type: IPv4

Mask on
    Source IP           : 255.255.255.255
    Destination IP     : 255.255.255.255
    DSCP

Available Hardware Entries : 126
------------------------------------------------------------------------------
Rule ID : 1    (auto assign)    Port group: 1

Match on
    Source IP           : 10.0.0.2
    Destination IP     : 10.90.90.90
    DSCP                : 25
```

```
Action:
    Permit

------------------------------------------------------------------------------
Rule ID : 2    (auto assign)    Port group: 1

Match on
    Source IP           : 10.0.0.1
    Destination IP     : 10.90.90.90
    DSCP                 : 25

Action:
    Permit

Matched Count : 0 packets
==============================================================================

DWS-3160-24PC:admin#
```

The following example displays an egress access profile that supports an entry mask for each rule:

```
DWS-3160-24PC:admin# show egress_access_profile profile_id 1
Command: show egress_access_profile profile_id 1

Egress Access Profile Table

==============================================================================
Profile ID: 1     Profile name: 1  Type: Ethernet

Mask on
    Source MAC      : FF-FF-FF-FF-FF-FF

Available Hardware Entries : 127
------------------------------------------------------------------------------
Rule ID : 1       Port group: -

Match on
    VLAN ID         : 1
    Source MAC      : 00-00-00-00-00-01

Action:
    Permit

==============================================================================
DWS-3160-24PC:admin#
```

7-5 show current_config egress_access_profile

Description

This command is used to display the egress ACL part of current configuration in user level of privilege. The overall current configuration can be displayed by “show config” command which is accessible in administrator level of privilege.

Format

show current_config egress_access_profile

Parameters

None.

Restrictions

None.

Example

To display current configuration of egress access list table:

```
DWS-3160-24PC:admin# show current_config egress_access_profile
Command: show current_config egress_access_profile

#-----------------------------------------------------------------------------

# Egress ACL

create egress_access_profile profile_id 1 profile_name 1 ethernet source_mac
FF-FF-FF-FF-FF-FF
config egress_access_profile profile_id 1 add access_id 1 ethernet source_mac
00-00-00-00-00-01 vlan_based vlan_id 1 permit
create egress_access_profile profile_id 2 profile_name 2 ip source_ip_mask
255.255.255.255 destination_ip_mask 255.255.255.255 dscp
config egress_access_profile profile_id 2 add access_id auto_assign ip
source_ip 10.0.0.2 destination_ip 10.90.90.90 dscp 25 port_group id 1 permit
counter enable
config egress_access_profile profile_id 2 add access_id auto_assign ip
source_ip 10.0.0.1 destination_ip 10.90.90.90 dscp 25 port_group id 1 permit

#-----------------------------------------------------------------------------

DWS-3160-24PC:admin#
```

7-6 config egress_flow_meter

Description

This command is used to configure the packet flow-based metering based on an egress access profile and rule.

Format

config egress_flow_meter [profile_id <value 1-4> | profile_name <name 1-32>] access_id <value 1-128> [rate [<value>] {burst_size [<value>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value> {cbs <value>} pir <value> {pbs <value>} {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter

[enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | sr_tcm cir <value> cbs <value> ebs <value> {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | delete]

Parameters

profile_id - Specifies the profile ID.
<value 1-4> - Enter the profile ID used here. This value must be between 1 and 4.

profile_name - Specifies the name of the profile. The maximum length is 32 characters.
<name> - Enter the profile name used here.

access_id - Specifies the access ID.
<value 1-128> - Enter the access ID used here. This value must be between 1 and 128.

rate - This specifies the rate for single rate two-color mode. Specifies the committed bandwidth in Kbps for the flow.
<value> - Enter the rate for single rate two-color mode here.

burst_size - (Optional) This specifies the burst size for the single rate “two color” mode. The unit is Kbytes.
<value> - Enter the burst size value here.

rate_exceed - This specifies the action for packets that exceed the committed rate in single rate “two color” mode. The action can be specified as one of the following:
drop_packet - Drop the packet immediately.
remark_dscp - Mark the packet with a specified DSCP. The packet is set to have the higher drop precedence.
<value 0-63> - Enter the remark DSCP value here. This value must be between 0 and 63.

tr_tcm - Specifies the “two rate three color mode”.
<value> - Enter the two rate three color mode value here.

cbs - (Optional) Specifies the “Committed Burst Size”. The unit is Kbytes. That is to say, 1 means 1Kbytes. This parameter is an optional parameter. The default value is 4*1024.
<value> - Enter the committed burst size value here.

pir - Specifies the “Peak Information Rate”. The unit is in Kbps. PIR should always be equal to or greater than CIR.
<value> - Enter the peak information rate value here.

pbs - (Optional) Specifies the “Peak Burst Size”. The unit is in Kbytes.
<value> - Enter the peak burst size value here.

color_blind - (Optional) Specifies the meter mode to be color-blind. The default is color-blind mode.
color_aware - (Optional) Specifies the meter mode to be color-aware. When this code is specified, user could set the “in-coming packet color” by using command “config color_aware”. The final color of packet is determined by the initial color of packet and the metering result.

conform - (Optional) Specifies the action when packet is in “green color”.
permit - Permit the packet.
replace_dscp - Changes the DSCP of the packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.

counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
enable - Specifies that the ACL counter parameter will be enabled.
disable - Specifies that the ACL counter parameter will be disabled.

exceed - Specifies the action when packet is in “yellow color”.

permit - (Optional) Permit the packet.
replace_dscp - Changes the DSCP of the packet.
<value 0-63> - Enter the DSCP replace value here. This value must be between 0 and 63.
drop - Drops the packet.

counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when

the function is disabled. **enable** - Specifies that the ACL counter parameter will be enabled. **disable** - Specifies that the ACL counter parameter will be disabled.
violate - Specifies the action when packet is in “red color”.
permit - Permit the packet. **replace_dscp** - (Optional) Changes the DSCP of the packet. **<value 0-63>** - Enter the DSCP replace value here. This value must be between 0 and 63. **drop** - Drops the packet.
counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled. **enable** - Specifies that the ACL counter parameter will be enabled. **disable** - Specifies that the ACL counter parameter will be disabled.
sr_tcm - Specifies the “single rate three color mode”. **<value>** - Enter the single rate three color mode value here.
cbs - Specifies the “committed burst size”. The unit is Kbytes. **<value>** - Enter the committed burst size value here.
ebs - Specifies the “Excess Burst Size”. The unit is Kbytes. **<value>** - Enter the excess burst size value here.
color_blind - (Optional) Specifies the meter mode to be color-blind. The default is color-blind mode. **color_aware** - (Optional) Specifies the meter mode to be color-aware. When this code is specified, user could set the “in-coming packet color” by using command “config color_aware”. The final color of packet is determined by the initial color of packet and the metering result.
conform - (Optional) Specifies the action when packet is in “green color”.
permit - (Optional) Permit the packet. replace_dscp - Changes the DSCP of the packet. **<value 0-63>** - Enter the replace DSCP value here. This value must be between 0 and 63.
counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled. **enable** - Specifies that the ACL counter parameter will be enabled. **disable** - Specifies that the ACL counter parameter will be disabled.
exceed - Specifies the action when packet is in “yellow color”.
permit - Permit the packet. **replace_dscp** - (Optional) Changes the DSCP of the packet. **<value 0-63>** - Enter the DSCP replace value here. This value must be between 0 and 63. **drop** - Drops the packet.
counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled. **enable** - Specifies that the ACL counter parameter will be enabled. **disable** - Specifies that the ACL counter parameter will be disabled.
violate - Specifies the action when packet is in “red color”.
permit - Permit the packet. **replace_dscp** - (Optional) Changes the DSCP of the packet. **<value 0-63>** - Enter the DSCP replace value here. This value must be between 0 and 63. **drop** - Drops the packet.
counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled. **enable** - Specifies that the ACL counter parameter will be enabled. **disable** - Specifies that the ACL counter parameter will be disabled.
delete - Delete the specified “flow_meter”.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a “two rates three color” flow meter:

```
DWS-3160-24PC:admin# config egress_flow_meter profile_id 1 access_id 1 tr_tcm
cir 1000 cbs 200 pir 2000 pbs 200 exceed replace_dscp 21 violate drop
command: config egress_flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs
200 pir 2000 pbs 200 exceed replace_dscp 21 violate drop


Success.


DWS-3160-24PC:admin#
```

7-7 show egress_flow_meter

Description

This command is used to display the egress flow-based metering configuration.

Format

show egress_flow_meter {[profile_id <value 1-4> | profile_name <name 1-32>] {access_id <value 1-128>}}

Parameters

profile_id - (Optional) Specifies the index of access list profile.
    <value 1-4> - Enter the profile ID used here. This value must be between 1 and 4.

profile_name - (Optional) Specifies the name of the profile.
    <name 1-32> - Enter the profile name used here. This name can be up to 32 characters long.

access_id - (Optional) Specifies the access ID.
    <value 1-128> - Enter the access ID used here. This value must be between 1 and 128.

Restrictions

None.

Example

To display current egress flow meter table:

```
DWS-3160-24PC:admin#show egress_flow_meter
Command: show egress_flow_meter

Flow Meter Information
------------------------------------------------------------------------------
Profile ID:1     Access ID:1     Mode : trTCM / ColorAware
CIR(Kbps):1000     CBS(Kbyte):1000     PIR(Kbps):2000     PBS(Kbyte):2000
Action:
      Conform : Permit                        Counter: Enabled
       Exceed : Drop                          Counter: Enabled
      Violate : Drop                          Counter: Disabled
------------------------------------------------------------------------------
Profile ID:1     Access ID:2     Mode : srTCM / ColorBlind
CIR(Kbps):1000     CBS(Kbyte):100      EBS(Kbyte):200
Action:
      Conform : Permit                        Counter: Enabled
       Exceed : Permit     Replace DSCP: 60   Counter: Enabled
      Violate : Drop                          Counter: Disabled
------------------------------------------------------------------------------

Total Entries: 2

DWS-3160-24PC:admin#
```

7-8 create port_group

Description

This command is used to create a port group.

Format

create port_group id <value 1-64> name <name 16>

Parameters

id - Specifies the port group ID.
<value 1-64> - Enter the port group ID here. This value must be between 1 and 64.

name - Specifies the port group name.
<name 16> - Enter the port group name here. This name can be up to 16 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a port group:

```
DWS-3160-24PC:admin# create port_group id 2 name group2
Command: create port_group id 2 name group2

Success.

DWS-3160-24PC:admin#
```

7-9 config port_group

Description

This command is used to add or delete a port list to a port group.

Format

config port_group [id <value 1-64> | name <name 16>] [add | delete] [<portlist> | all]

Parameters

id - Specifies the port group ID.
<value 1-64> - Enter the port group ID used here. This value must be between 1 and 64.

name - Specifies the port group name.
<name 16> - Enter the port group name here. This name can be up to 16 characters long.

add - Add a port list to this port group.
delete - Delete a port list from this port group.

<portlist> - Enter a list of ports used for the configuration here.
all - Specifies that all the ports will be used for this configuration.

Restrictions

Only Administrators and Operators can issue this command.

Example

Add port list “1-3” to the port group which ID is “2”:

```
DWS-3160-24PC:admin# config port_group id 2 add 1-3
Command: config port_group id 2 add 1-3

Success.

DWS-3160-24PC:admin#
```

7-10 delete port_group

Description

This command is used to delete port group.

Format

delete port_group [id <value 1-64> | name <name 16>]

Parameters

id - Specifies the port group ID.
<value 1-64> - Enter the port group ID used here. This value must be between 1 and 64.

name - Specifies the port group name.
<name 16> - Enter the port group name here. This name can be up to 16 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the port group which ID is “2”:

```
DWS-3160-24PC:admin# delete port_group id 2
Command: delete port_group id 2

Success.

DWS-3160-24PC:admin#
```

7-11 show port_group

Description

This command is used to display the port group information.

Format

show port_group {id<value 1-64> | name<name 16>}

Parameters

id - (Optional) Specifies the port group ID.
<value 1-64> - Enter the port group ID used here. This value must be between 1 and 64.

name - (Optional) Specifies the port group name.
<name 16> - Enter the port group name here. This name can be up to 16 characters long.

If not specified parameter, will display all the port group.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display all the port group information:

```
DWS-3160-24PC:admin# show port_group
Command: show port_group

Port Group Table
Group ID     Group Name                        Ports
1              group1                          1-2,5
2              group2                          4-5,7,9,11,13
                                               15,17,19-25
4              group3                          5-7

Total Entries :3

DWS-3160-24PC:admin#
```

Chapter 8 Address Resolution Protocol (ARP) Command List

create arpentry <ipaddr> <macaddr>
delete arpentry [<ipaddr> | all]
config arpentry <ipaddr> <macaddr>
config arp_aging time <minutes 0-65535>
clear arptable
show arpentry {ipif <ipif_name 12> **|** ipaddress <ipaddr> **|** static | mac_address <macaddr>}

8-1 create arpentry

Description

This command is used to enter a static ARP entry into the Switch's ARP table.

Format

create arpentry <ipaddr> <macaddr>

Parameters

<ipaddr> - The IP address of the end node or station.
<macaddr> - The MAC address corresponding to the IP address above.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a static ARP entry for the IP address 10.48.74.121 and MAC address 00-50-BA-00-07-36:

```
DWS-3160-24PC:admin# create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

DWS-3160-24PC:admin#
```

8-2 delete arpentry

Description

This command is used to delete an ARP entry, by specifying either the IP address of the entry or all. Specifies 'all' clears the Switch's ARP table.

Format

delete arpentry [<ipaddr> | all]

Parameters

<ipaddr> - The IP address of the end node or station.

all - Delete all ARP entries.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an entry of IP address 10.48.74.121 from the ARP table:

```
DWS-3160-24PC:admin# delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DWS-3160-24PC:admin#
```

8-3 config arpentry

Description

This command is used to configure a static entry’s MAC address in the ARP table. Specifies the IP address and MAC address of the entry.

Format

config arpentry <ipaddr> <macaddr>

Parameters

<ipaddr> - The IP address of the end node or station.

<macaddr> - The MAC address corresponding to the IP address above.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a static ARP entry, whose IP address is 10.48.74.121, set its MAC address to 00-50-BA-00-07-37:

```
DWS-3160-24PC:admin# config arpentry 10.48.74.121 00-50-BA-00-07-37
Command: config arpentry 10.48.74.121 00-50-BA-00-07-37

Success.

DWS-3160-24PC:admin#
```

8-4 config arp_aging time

Description

This command is used to configure the maximum amount of time, in minutes, that a dynamic ARP entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table.

Format

config arp_aging time <minutes 0-65535>

Parameters

time - The ARP age-out time, in minutes, the default is 20.

<minutes 0-65535> - Enter the ARP age-out time here. This value must be between 0 and 65535 minutes.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure ARP aging time to 30 minutes:

```
DWS-3160-24PC:admin# config arp_aging time 30
Command: config arp_aging time 30

Success.

DWS-3160-24PC:admin#
```

8-5 clear arptable

Description

This command is used to clear all the dynamic entries from ARP table.

Format

clear arptable

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear the ARP table:

```
DWS-3160-24PC:admin# clear arptable
Command: clear arptable

Success.

DWS-3160-24PC:admin#
```

8-6 show arpentry

Description

This command is used to displays the ARP table. You can filter the display by IP address, MAC address, Interface name, or static entries.

Format

show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static | mac_address <macaddr>}

Parameters

ipif - (Optional) The name of the IP interface the end node or station for which the ARP table entry was made, resides on.
    <ipif_name 12> - Enter the IP interface name here. This value can be up to 12 characters long.

ipaddress - (Optional) The IP address of the end node or station.
    <ipaddr> - Enter the IP address here.

static - (Optional) Display the static entries in the ARP table.

mac_address - (Optional) Displays the ARP entry by MAC address.
    <macaddr> - Enter the MAC address here.

Restrictions

None.

Example

To display the ARP table:

```
DWS-3160-24PC:admin#show arpentry
Command: show arpentry

 ARP Aging Time : 30

Interface      IP Address       MAC Address        Type
-------------  ---------------  -----------------  ---------------
System         10.0.0.0         FF-FF-FF-FF-FF-FF  Local/Broadcast
System         10.48.74.121     00-50-BA-00-07-37  Static
System         10.90.90.20      00-22-B0-3C-DD-C0  Dynamic
System         10.90.90.90      00-11-22-33-45-67  Local
System         10.90.90.91      00-11-22-33-32-32  Dynamic
System         10.255.255.255   FF-FF-FF-FF-FF-FF  Local/Broadcast

Total Entries: 6

DWS-3160-24PC:admin#
```

Chapter 9 ARP Spoofing Prevention Command List

config arp_spoofing_prevention [add gateway_ip <ipaddr> gateway_mac <macaddr> ports [<portlist> | all] | delete gateway_ip <ipaddr>]

show arp_spoofing_prevention

9-1 config arp_spoofing_prevention

Description

This command is used to configure the spoofing prevention entry to prevent spoofing of MAC for the protected gateway. When an entry is created, those ARP packets whose sender IP matches the gateway IP of an entry, but either its sender MAC field or source MAC field doesn't match the gateway MAC of the entry will be dropped by the system.

Format

config arp_spoofing_prevention [add gateway_ip <ipaddr> gateway_mac <macaddr> ports [<portlist> | all] | delete gateway_ip <ipaddr>]

Parameters

add - Specifies to add an ARP spoofing prevention entry.
gateway_ip - Specifies a gateway IP address to be configured. **<ipaddr>** - Enter the IP address used for this configuration here.
gateway_mac - Specifies a gateway MAC address to be configured. **<macaddr>** - Enter the MAC address used for this configuration here.
ports - Specifies a range of ports to be configured. **<portlist>** - Enter a list of ports used for the configuration here. **all** - Specifies all of ports to be configured.
delete - Specifies to delete an ARP spoofing prevention entry.
gateway_ip - Specifies a gateway ip to be configured. **<ipaddr>** - Enter the IP address used for this configuration here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the ARP spoofing prevention entry:

```
DWS-3160-24PC:admin# config arp_spoofing_prevention add gateway_ip
10.254.254.251 gateway_mac 00-00-00-11-11-11 ports 1-2
Command: config arp_spoofing_prevention add gateway_ip 10.254.254.251
gateway_mac 00-00-00-11-11-11 ports 1-2

Success.

DWS-3160-24PC:admin#
```

9-2 show arp_spoofing_prevention

Description

This command is used to display the ARP spoofing prevention entry.

Format

show arp_spoofing_prevention

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display the ARP spoofing prevention entries:

```
DWS-3160-24PC:admin#show arp_spoofing_prevention
Command: show arp_spoofing_prevention

Gateway IP         Gateway MAC          Ports
------------------ -------------------  --------------------
10.254.254.251     00-00-00-11-11-11    1-2

 Total Entries: 1

DWS-3160-24PC:admin#
```

Chapter 10 Asymmetric VLAN Command List

enable asymmetric_vlan
disable asymmetric_vlan
show asymmetric_vlan

10-1 enable asymmetric_vlan

Description

This command is used to enable the asymmetric VLAN function on the Switch.

Format

enable asymmetric_vlan

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable asymmetric VLANs:

```
DWS-3160-24PC:admin# enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

DWS-3160-24PC:admin#
```

10-2 disable asymmetric_vlan

Description

This command is used to disable the asymmetric VLAN function on the Switch.

Format

disable asymmetric_vlan

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable asymmetric VLANs:

```
DWS-3160-24PC:admin# disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.

DWS-3160-24PC:admin#
```

10-3 show asymmetric_vlan

Description

This command is used to display the asymmetric VLAN state on the Switch.

Format

show asymmetric_vlan

Parameters

None.

Restrictions

None.

Example

To display the asymmetric VLAN state currently set on the Switch:

```
DWS-3160-24PC:admin#show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric VLAN : Enabled

DWS-3160-24PC:admin#
```

Chapter 11 Auto-Configuration Command List

enable autoconfig

disable autoconfig

show autoconfig

11-1 enable autoconfig

Description

This command is used to enable the automatic configuration feature of this Switch. When automatic configuration is enabled, during power on initialization, the Switch will get configure file path name and TFTP server IP address from the DHCP server. Then, the Switch will download the configuration file from the TFTP server for configuration of the system.

Format

enable autoconfig

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable autoconfig:

```
DWS-3160-24PC:admin# enable autoconfig
Command: enable autoconfig

Success.

DWS-3160-24PC:admin#
```

11-2 disable autoconfig

Description

This command is used to disable the automatic configuration feature of this Switch. When auto configuration is disabled, the Switch will configure itself using the local configuration file

Format

disable autoconfig

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable autoconfig:

```
DWS-3160-24PC:admin# disable autoconfig
Command: disable autoconfig

Success.

DWS-3160-24PC:admin#
```

11-3 show autoconfig

Description

This command is used to display if the auto-configuration is enabled or disabled.

Format

show autoconfig

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To display autoconfig status:

```
DWS-3160-24PC:admin#show autoconfig
Command: show autoconfig

Autoconfig State: Enabled

DWS-3160-24PC:admin#
```

Chapter 12 Basic Commands Command List

create account [admin | operator | power_user | user] <username 15> {encrypt [plain_text | sha_1] <password>}

config account <username> {encrypt [plain_text | sha_1] <password>}

show account

delete account <username>

show switch

enable telnet {<tcp_port_number 1-65535>}

disable telnet

enable web {<tcp_port_number 1-65535>}

disable web

reboot {force_agree}

reset {[config | system]} {force_agree}

config firmware image <path_filename 64> boot_up

create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {secondary | state [enable | disable] | proxy_arp [enable | disable] {local [enable | disable]}}

config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | proxy_arp [enable | disable] {local [enable | disable]} | state [enable | disable]} | bootp | dhcp |ipv6 [ipv6address <ipv6networkaddr> | state [enable | disable]] | ipv4 state [enable | disable]]

delete ipif [<ipif_name 12> {ipv6address <ipv6networkaddr>} | all]

enable ipif [<ipif_name 12> | all]

disable ipif [<ipif_name 12> | all]

show ipif {<ipif_name 12>}

enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

show ipif_ipv6_link_local_auto {<ipif_name 12>}

12-1 create account

Description

This command is used to create user accounts. It is case sensitive. The number of account (include admin and user) is up to 8.

Format

create account [admin | operator | power_user | user] <username 15> {encrypt [plain_text | sha_1] <password>}

Parameters

admin - Specifies the name of the admin account.
operator - Specifies the name for a operator user account.
power_user – Specifies the name for a Power-user account.
user - Specifies the name of the user account.
<username 15> - Enter the username used here. This name can be up to 15 characters long.

encrypt - (Optional) Specifies the encryption applied to the account.
plain_text - Select to Specifies the password in plain text form.
sha_1 - Select to Specifies the password in the SHA-I encrypted form.
<password> - The password for the user account. The length for of password in plain-text

form and in encrypted form are different. For the plain-text form, passwords must have a minimum of 0 character and can have a maximum of 15 characters. For the encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive.

Restrictions

Only Administrators can issue this command.

Example

To create the admin-level user “dlink”:

```
DWS-3160-24PC:admin# create account admin dlink
Command: create account admin dlink

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****

Success.

DWS-3160-24PC:admin#
```

To create the user-level user “Remote-Manager”:

```
DWS-3160-24PC:admin# create account user Remote-Manager
Command: create account user Remote-Manager

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****

Success.

DWS-3160-24PC:admin#
```

12-2 config account

Description

This command is used to configure a user account created on this Switch. When the password information is not specified in the command, the system will prompt the user to input the password interactively. For this case, the user can only input the plain text password.

If the password is present in the command, the user can select to input the password in the plain text form or in the encrypted form. The encryption algorithm is based on SHA-I.

Format

config account <username> {encrypt [plain_text | sha_1] <password>}

Parameters

account - Name of the account. The account must already be defined.
<username> - Enter the user name for the account used here.

encrypt - (Optional) Specifies that the password will be encrypted.
- **plain_text** - Select to Specifies the password in plain text form.
- **sha_1** - Select to Specifies the password in the SHA-1 encrypted form.
  - **<password>** - The password for the user account. The length for of password in plain-text form and in encrypted form are different. For the plain-text form, passwords must have a minimum of 0 character and can have a maximum of 15 characters. For the encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive.

Restrictions

Only Administrators can issue this command.

Example

To configure the user password of “dlink” account:

```
DWS-3160-24PC:admin# config account dlink
Command: config account dlink

Enter a old password:****
Enter a case-sensitive new password:****
Enter the new password again for confirmation:****

Success.

DWS-3160-24PC:admin#
```

To configure the user password of “superuser” account using the SHA-1 encryption:

```
DWS-3160-24PC:admin#config account superuser encrypt sha_1
*@&jme7JrNY4u0g/lUu1vuDLzl6UH1zNMbt
Command: config account superuser encrypt sha_1
*@&jme7JrNY4u0g/lUu1vuDLzl6UH1zNMbt

Success.

DWS-3160-24PC:admin#
```

12-3 show account

Description

This command is used to display user accounts that have been created.

Format

show account

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display the accounts that have been created:

```
DWS-3160-24PC:admin#show account
Command: show account

 Current Accounts:
 Username             Access Level
 ---------------      ------------
 admin                Admin
 operator             Operator
 power                Power_user
 user                 User

 Total Entries : 4

DWS-3160-24PC:admin#
```

12-4 delete account

Description

This command is used to delete an existing account.

Format

delete account <username>

Parameters

<username> - Name of the user who will be deleted.

Restrictions

Only Administrators can issue this command.

Example

To delete the user account “System”:

```
DWS-3160-24PC:admin# delete account System
Command: delete account System

Success.

DWS-3160-24PC:admin#
```

12-5 show switch

Description

This command is used to display the Switch information.

Format

show switch

Parameters

None.

Restrictions

None.

Example

The following is an example for display of Switch information.

```
DWS-3160-24PC:admin#show switch
Command: show switch

Device Type                : DWS-3160-24PC Gigabit Ethernet Switch
MAC Address                : 00-01-02-03-04-00
IP Address                 : 10.90.90.90 (Manual)
VLAN Name                  : default
Subnet Mask                : 255.0.0.0
Default Gateway            : 0.0.0.0
Boot PROM Version          : Build 1.00.001
Firmware Version           : Build 1.00.034
Hardware Version           : A1
System Name                :
System Location            :
System Uptime              : 0 days, 3 hours, 0 minutes, 36 seconds
System Contact             :
Spanning Tree              : Disabled
GVRP                       : Disabled
IGMP Snooping              : Disabled
MLD Snooping               : Disabled
VLAN Trunk                 : Disabled
Telnet                     : Enabled (TCP 23)
Web                        : Enabled (TCP 80)
SNMP                       : Disabled
SSL Status                 : Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

12-6 enable telnet

Description

This command is used to enable the Switch's TELNET based management software.

Format

enable telnet {<tcp_port_number 1-65535>}

Parameters

<tcp_port_number 1-65535> - (Optional) The TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the TELNET protocol is 23.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable TELNET and configure port number:

```
DWS-3160-24PC:admin# enable telnet 23
Command: enable telnet 23

Success.

DWS-3160-24PC:admin#
```

12-7 disable telnet

Description

This command is used to disable the Switch's TELNET based management software.

Format

disable telnet

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable TELNET:

```
DWS-3160-24PC:admin# disable telnet
Command: disable telnet

Success.

DWS-3160-24PC:admin#
```

12-8 enable web

Description

This command is used to enable the Switch’s HTTP based management software.

Format

enable web {<tcp_port_number 1-65535>}

Parameters

<tcp_port_number 1-65535> - (Optional) The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the WEB protocol is 80.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable HTTP and configure port number:

```
DWS-3160-24PC:admin# enable web 80
Command: enable web 80

Success.

DWS-3160-24PC:admin#
```

12-9 disable web

Description

This command is used to disable the Switch’s HTTP based management software.

Format

disable web

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable HTTP:

```
DWS-3160-24PC:admin# disable web
Command: disable web

Success.

DWS-3160-24PC:admin#
```

12-10 reboot

Description

This command is used to reboot the Switch.

Format

reboot {force_agree}

Parameters

force_agree - (Optional) When force_agree is specified, the reboot command will be executed immediately without further confirmation.

Restrictions

Only Administrators can issue this command.

Example

To reboot the Switch:

```
DWS-3160-24PC:admin# reboot
Command: reboot

Are you sure to proceed with the system reboot?(y/n)
Please wait, the switch is rebooting…
```

12-11 reset

Description

This command is used to reset the Switch. The configuration setting will be reset to the default setting. For the “save system” command, the device will store the reset setting in the NVRAM and then reboot the system.

The configuration settings include enable/disable of clipaging, greeting message, and command prompt will also be reset by all the reset commands.

There is one exception, the “reset” command will not reset IP address configured on the system IPIF and the default gateway setting.

Format

reset {[config | system]} {force_agree}

Parameters

config - (Optional) If you Specifies the ‘config’ keyword , all parameters are reset to default settings. But device will not do save neither reboot.

system - (Optional) If you Specifies the ‘system’ keyword, all parameters are reset to default settings. Then the Switch will do factory reset, save and reboot.

force_agree - (Optional) When force_agree is specified, the reset command will be executed immediately without further confirmation.

Restrictions

Only Administrators can issue this command.

Example

To reset the Switch:

```
DWS-3160-24PC:admin#reset system
Command: reset system

Are you sure you want to proceed with system reset?(y/t/n)
 y-(reset all include stacking configuration, save, reboot )
 t-(reset all exclude stacking configuration, save, reboot)
 n-(cancel command)y

Reboot & Load Factory Default Configuration...

Saving configurations and logs to NV-RAM...... Done.
Please wait, the switch is rebooting...
```

12-12 config firmware

Description

This command is used to select a firmware file as the boot-up file.

Format

config firmware image <path_filename 64> boot_up

Parameters

<path_filename 64> - Specifies a firmware file on the device file system.

boot_up - Specifies the firmware as the boot up firmware.

Restrictions

Only Administrators can issue this command.

Example

To config image 1 as the boot up image:

```
DWS-3160-24PC:admin# config firmware image image1 boot_up
Command: config firmware image image1 boot_up

Success.

DWS-3160-24PC:admin#
```

12-13 create ipif

Description

This command is used to create an IP interface.

Format

create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {secondary | state [enable | disable] | proxy_arp [enable | disable] {local [enable | disable]}}

Parameters

ipif - Specifies the name of the IP interface.
  <ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.

<network_address> - (Optional) Enter the network address used here.

<vlan_name 32> - Enter the VLAN name used here. This name can be up to 32 characters long.

secondary - (Optional) Specifies the IPv4 secondary interface to be created.

state - (Optional) Specifies the state of the IP interface.
  enable - Specifies that the IP interface state will be enabled.
  disable - Specifies that the IP interface state will be disabled.

proxy_arp - (Optional) Enable or disable of proxy ARP function. It is for IPv4 function. Default: Disabled.
  enable - Specifies that the proxy ARP option will be enabled.
  disable - Specifies that the proxy ARP option will be disabled.

local - (Optional) This setting controls whether the system provides the proxy reply for the ARP packets destined for IP address located in the same interface as the received interface. When proxy ARP is enabled for an interface, the system will do the proxy reply for the ARP packets destined for IP address located in a different interface. For ARP packets destined for IP address located in the same interface, the system will check this setting to determine whether to reply.
  enable - Specifies that the local option will be enabled.
  disable - Specifies that the local option will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an IP interface:

```
DWS-3160-24PC:admin#create ipif Inter2 192.168.16.1/24 default state enable
secondary
Command: create ipif Inter2 192.168.16.1/24 default state enable secondary

Success.

DWS-3160-24PC:admin#
```

12-14 config ipif

Description

This command is used to configure the IP interface.

Format

config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | proxy_arp [enable | disable] {local [enable | disable]} | state [enable | disable]} | bootp | dhcp |ipv6 [ipv6address <ipv6networkaddr> | state [enable | disable]] | ipv4 state [enable | disable]]

Parameters

ipif - Specifies the name of the IP interface.
<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

ipaddress - Configures a network on an ipif. The address should Specifies a host address and length of network mask. Since an ipif can have only one IPv4 address, the new configured address will overwrite the original one.
<network_address> - Enter the network address used here.

vlan - Specifies the name of the VLAN here.
<vlan_name 32> - Enter the VLAN name used here. This name can be up to 32 characters long.

proxy_arp - Enable/disable of proxy ARP function. It is for IPv4 function. Default: Disabled.
enable - Specifies that the proxy ARP option will be enabled.
disable - Specifies that the proxy ARP option will be disabled.

local - This setting controls whether the system provides the proxy reply for the ARP packets destined for IP address located in the same interface as the received interface. When proxy ARP is enabled for an interface, the system will do the proxy reply for the ARP packets destined for IP address located in a different interface. For ARP packets destined for IP address located in the same interface, the system will check this setting to determine whether to reply.
enable - Specifies that the local option will be enabled.
disable - Specifies that the local option will be disabled.

bootp - Use BOOTP to obtain the IPv4 address.

dhcp - Use DHCP to obtain the IPv4 address.

ipv6 - Specifies that the IPv6 configuration will be done.
ipv6address - Specifies the IPv6 network address. The address should Specifies a host

address and length of network prefix. There can be multiple V6 addresses defined on an interface. Thus, as a new address is defined, it is added on this ipif.
<ipv6networkaddr> - Enter the IPv6 address used here.

state - Specifies that the IPv6 interface state will be set to enabled or disabled.
enable - Specifies that the IPv6 interface sate will be enabled.
disable - Specifies that the IPv6 interface sate will be disabled.

ipv4 - Specifies that the IPv4 configuration will be done.

state - Specifies that the IPv4 interface state will be set to enabled or disabled.
enable - Specifies that the IPv4 interface sate will be enabled.
disable - Specifies that the IPv4 interface sate will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure an interface's IPv4 network address:

```
DWS-3160-24PC:admin#config ipif System ipaddress 192.168.69.123/24 vlan default
Command: config ipif System ipaddress 192.168.69.123/24 vlan default

Success.

DWS-3160-24PC:admin#
```

12-15 delete ipif

Description

This command is used to delete an IP interface.

Format

delete ipif [<ipif_name 12> {ipv6address <ipv6networkaddr>} | all]

Parameters

ipif - Specifies the name of the IP interface.
<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

ipv6address – (Optional) Specifies the IPv6 network address. The address should Specifies a host address and length of network prefix. There can be multiple V6 addresses defined on an interface.
<ipv6networkaddr> - Enter the IPv6 address used here.
all – Specifies that all the IP interfaces will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an IP interface:

```
DWS-3160-24PC:admin#delete ipif newone
Command: delete ipif newone

Success.

DWS-3160-24PC:admin#
```

12-16 enable ipif

Description

This commands is used to enable the IP interface.

Format

enable ipif [<ipif_name 12> | all]

Parameters

ipif_name - Specifies the name of the IP interface.
- **<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.
- **all** – Specifies that all the IP interfaces will be enabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable an IP interface:

```
DWS-3160-24PC:admin#enable ipif newone
Command: enable ipif newone

Success.

DWS-3160-24PC:admin#
```

12-17 disable ipif

Description

This command is used to disable an IP interface.

Format

disable ipif [<ipif_name 12> | all]

Parameters

ipif_name - Specifies the name of the IP interface.

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

all – Specifies that all the IP interfaces will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable an IP interface:

```
DWS-3160-24PC:admin#disable ipif newone
Command: disable ipif newone

Success.

DWS-3160-24PC:admin#
```

12-18 show ipif

Description

This command is used to display an IP interface.

Format

show ipif {<ipif_name 12>}

Parameters

ipif_name - Specifies the name of the IP interface.

<ipif_name 12> - (Optional) Enter the IP interface name used here. This name can be up to 12 characters long.

Restrictions

None.

Example

To display an IP interface:

```
DWS-3160-24PC:admin#show ipif
Command: show ipif

IP Interface                : Inter2
VLAN Name                   : default
Interface Admin State       : Enabled
Link Status                 : LinkUp
IPv4 Address                : 192.168.16.1/24 (Manual)  Secondary
Proxy ARP                   : Disabled   (Local : Disabled)
IPv4 State                  : Enabled

IP Interface                : System
VLAN Name                   : default
Interface Admin State       : Enabled
Link Status                 : LinkUp
IPv4 Address                : 10.90.90.90/8 (Manual)  Primary
Proxy ARP                   : Disabled   (Local : Disabled)
IPv4 State                  : Enabled
IPv6 State                  : Enabled

Total Entries: 2

DWS-3160-24PC:admin#
```

12-19 enable ipif_ipv6_link_local_auto

Description

This command is used to enable the automatic configuration of a link local address when there are no IPv6 addresses explicitly configured. When an IPv6 address is explicitly configured, the link local address will be automatically configured, and the IPv6 processing will be started. When there is no IPv6 address explicitly configured, by default, link local address is not configured and the IPv6 processing will be disabled. By enable this automatic configuration, the link local address will be automatically configured and IPv6 processing will be started.

Format

enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

all - Specifies that all the IP interfaces will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the IP interface for IPv6 link local automatic:

```
DWS-3160-24PC:admin#enable ipif_ipv6_link_local_auto newone
Command: enable ipif_ipv6_link_local_auto newone

Success.

DWS-3160-24PC:admin#
```

12-20 disable ipif_ipv6_link_local_auto

Description

This command is used to disable the auto configuration of link local address when no IPv6 address are configured.

Format

disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

all - Specifies that all the IP interfaces will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the IP interface for IPv6 link local automatic:

```
DWS-3160-24PC:admin#disable ipif_ipv6_link_local_auto newone
Command: disable ipif_ipv6_link_local_auto newone

Success.

DWS-3160-24PC:admin#
```

12-21 show ipif_ipv6_link_local_auto

Description

This commands is used to display the link local address automatic configuration state.

Format

show ipif_ipv6_link_local_auto {<ipif_name 12>}

Parameters

<ipif_name 12> - (Optional) Enter the Ip interface name used here. This name can be up to 12 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

T o display the link local address automatic configuration state.

```
DWS-3160-24PC:admin#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

 IPIF: System          Automatic Link Local Address: Enabled

DWS-3160-24PC:admin#
```

Chapter 13 BPDU Attack Protection Command List

config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown} (1)
config bpdu_protection recovery_timer [<sec 60-1000000> | infinite]
config bpdu_protection [trap | log] [none | attack_detected | attack_cleared | both]
enable bpdu_protection
disable bpdu_protection
show bpdu_protection {ports {<portlist>}}

13-1 config bpdu_protection ports

Description

This command is used to configure ports used by the BPDU protection function on the Switch. In generally, there are two states in BPDU protection function. One is normal state, and another is under attack state. The under attack state have three modes: drop, block, and shutdown. A BPDU protection enabled port will enter under attack state when it receives one STP BPDU packet. And it will take action based on the configuration. Thus, BPDU protection can only be enabled on STP-disabled port.

BPDU protection has high priority than FBPDU setting configured by configure STP command in determination of BPDU handling. That is, when FBPDU is configured to forward STP BPDU but BPDU protection is enabled, then the port will not forward STP BPDU.

Format

config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown]}(1)

Parameters

<portlist> - Specified a range of ports to be configured (port number).
all – Specified that all the port will be configured.
state – (Optional) Specified the BPDU protection state. The default state is disable **enable** – Specifies to enable BPDU protection. **disable** – Specifies to disable BPDU protection.
mode – (Optional) Specifies the BPDU protection mode. The default mode is shutdown **drop** - Drop all received BPDU packets when the port enters under_attack state. **block** - Drop all packets (include BPDU and normal packets) when the port enters under_attack state. **shutdown -** Shut down the port when the port enters under_attack state.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the port state and drop mode:

```
DWS-3160-24PC:admin# config bpdu_protection ports 1 state enable mode drop
Commands: config bpdu_protection ports 1 state enable mode drop

Success.

DWS-3160-24PC:admin#
```

13-2 config bpdu_protection recovery_interval

Description

This command is used to configure the BPDU protection recovery interval. When a port enters the ‘under attack’ state, it can be disabled or blocked based on the configuration. The state can be recovered manually or by the auto recovery mechanism. This command is used to configure the auto-recovery timer. To manually recover the port, the user needs to disable and re-enable the port.

Format

config bpdu_protection recovery_timer [<sec 60-1000000> | infinite]

Parameters

recovery_timer - Specifies the BPDU protection Auto-Recovery recovery_timer. The default value of recovery_timer is 60.

<sec 60 –1000000> - The timer (in seconds) used by the Auto-Recovery mechanism to recover the port. The valid range is 60 to 1000000.

infinite - The port will not be auto recovered.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the BPDU protection recovery_timer to 120 seconds for the entire Switch:

```
DWS-3160-24PC:admin# config bpdu_protection recovery_timer 120
Commands: config bpdu_protection recovery_timer 120

Success.

DWS-3160-24PC:admin#
```

13-3 config bpdu_protection

Description

This command is used to configure the BPDU protection trap state or state for the Switch.

Format

config bpdu_protection [trap | log] [none | attack_detected | attack_cleared | both]

Parameters

trap - To Specifies the trap state.
log - To Specifies the log state.

none - Neither attack_detected nor attack_cleared is trapped or logged.
attack_detected - Events will be logged or trapped when the BPDU attacks is detected.
attack_cleared - Events will be logged or trapped when the BPDU attacks is cleared.
both - The events of attack_detected and attack_cleared shall be trapped or logged.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To config the BPDU protection trap state as both for the entire Switch:

```
DWS-3160-24PC:admin# config bpdu_protection trap both
Commands: config bpdu_protection trap both

Success.

DWS-3160-24PC:admin#
```

13-4 enable bpdu_protection

Description

This command is used to enable the BPDU protection function globally for the Switch.

Format

enable bpdu_protection

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the BPDU protection function globally:

```
DWS-3160-24PC:admin# enable bpdu_protection
Commands: enable bpdu_protection

Success.

DWS-3160-24PC:admin#
```

13-5 disable bpdu_protection

Description

This command is used to disable the BPDU protection function globally for the Switch.

Format

disable bpdu_protection

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the BPDU protection function globally:

```
DWS-3160-24PC:admin# disable bpdu_protection
Commands: disable bpdu_protection

Success.

DWS-3160-24PC:admin#
```

13-6 show bpdu_protection

Description

This command is used to display the BPDU protection global configuration or per port configuration of the Switch and its current status.

Format

show bpdu_protection {ports {<portlist>}}

Parameters

ports - Specified a range of ports to be configured. **<portlist>** - Enter the portlist here.

Restrictions

None.

Example

To display the BPDU protection for the entire Switch:

```
DWS-3160-24PC:admin#show bpdu_protection
Command: show bpdu_protection

 BPDU Protection Global Settings
 ----------------------------------------
 BPDU Protection Status         : Enabled
 BPDU Protection Recover Time   : 120 seconds
 BPDU Protection Trap Status    : Both
 BPDU Protection Log Status     : Both

DWS-3160-24PC:admin#
```

To display the BPDU protection status ports 1-12:

```
DWS-3160-24PC:admin# show bpdu_protection ports 1-12
Commands: show bpdu_protection ports 1-12

Port     State          Mode          Status
------ ------------ ----------- ----------
1        Enabled        shutdown     Normal
2        Enabled        shutdown     Normal
3        Enabled        shutdown     Normal
4        Enabled        shutdown     Normal
5        Enabled        shutdown     Under Attack
6        Enabled        shutdown     Normal
7        Enabled        shutdown     Normal
8        Enabled        shutdown     Normal
9        Enabled        shutdown     Normal
10       Enabled        Block        Normal
11       Disabled       shutdown     Normal
12       Disabled       shutdown     Normal

DWS-3160-24PC:admin#
```

Chapter 14 Cable Diagnostics Command List

cable_diag ports [<portlist> | all]

14-1 cable_diag ports

Description

This command is used to run a cable diagnostics report for all the ports or only for selected ports on this Switch. For Fast Ethernet ports, two pairs of the cable will be diagnosed. For Gigabit Ethernet ports, four pairs of the cable will be diagnosed. The type of cable error can be open, short, or crosstalk.

1. Open means that the cable in the error pair does not have a connection at the specified position.
2. Short means that the cables in the error pair has a short problem at the specified position,
3. Crosstalk means that the cable in the error pair has a crosstalk problem at the specified position.

When a port is in link-up status, the test will obtain the distance of the cable. Since the status is link-up, the cable will not have the short or open problem. But the test may still detect the crosstalk problem.

When a port is in link-down status, the link-down may be caused by many factors.

- When the port has a normal cable connection, but the remote partner is powered off, the cable diagnosis can still diagnose the health of the cable as if the remote partner is powered on.
- When the port does not have any cable connection, the result of the test will indicate no cable.
- The test will detect the type of error and the position where the error occurs.

NOTE: This test will consume a low number of packets. Since this test is for copper cables, the ports with fiber cables will be skipped from the test. For combo port, the test will always be applied to the copper media only.

Format

cable_diag ports [<portlist> | all]

Parameters

<portlist> - Enter a list of ports used for the configuration here.
all – Specifies that all the ports will be used for this configuration.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

Test the cable on port 1, 2, 3, 23 and 24:

```
DWS-3160-24PC:admin#cable_diag ports 1,2,3,23,24
Command: cable_diag ports 1-3,23-24

Perform Cable Diagnostics ...

Port      Type      Link Status    Test Result                   Cable Length (M)
------  ----------  -------------  -------------------------  -----------------
1       1000BASE-T  Link Up        OK                                1
2       1000BASE-T  Link Up        OK                                1
3       1000BASE-T  Link Down      Pair 1 Open      at   3M          -
                                   Pair 2 Open      at   3M
                                   Pair 3 Open      at   3M
                                   Pair 4 Open      at   3M
23      1000BASE-T  Link Up        OK                                4
24      1000BASE-T  Link Down      No Cable                          -

DWS-3160-24PC:admin#
```

Chapter 15 Captive Portal Command List

enable captive_portal

disable captive_portal

config captive_portal [http_port [<int 0-65535> | default] | https_port [<int 0-65535> | default] | statistics_interval [0 | <int 15-3600> | default] | authentication_timeout [<int 60-600> | default]]

config captive_portal trap [enable | disable] [all | client_auth_failure | client_connect | client_disconnect | client_db_full]

show captive_portal {[status | trap]}

create captive_portal configuration <int 1-10>

delete captive_portal configuration <int 1-10>

config captive_portal configuration <int 1-10>[background_color [<string 32> | default] | block [enable | disable] | clear | state [enable | disable] | foreground_color [<string 32> | default] | group [<int 1-10> | default] | idle_timeout [<int 0-900> | default] | interface [phy_port <portlist> | wireless_network <int 1-64>] [enable | disable] | locale <int 1-5> [accept_msg <string 512> | accept_text {<string 512>} | account_image <string 32> | account_label {<string 256>} | aup_text {<string 32768>} | background_image <string 32> | branding_image <string 32> | browser_title {<string 512>} | button_label <string 128> | code <string 32> | denied_msg <string 512> | font_list {<sentence>} | instructional_text {<string 1024>} | link <string 512> | logout_browser_title {<string 512>} | logout_button_label <string 128> | logout_confirmation_text {<string 512>} | logout_success_background_image <string 32> | logout_success_browser_title {<string 512>} | logout_success_text {<string 1024>} | logout_success_title {<string 512>} | logout_text {<string 1024>} | logout_title {<string 512>} | password_label {<string 128>} | popup_text {<string 512>} | resource_msg <string 512> | script_text {<string 512>} | timeout_msg <string 512> | title_text {<string 512>} | user_label {<string 128>} | welcome_text {<string 1024>} | welcome_title {<string 512>} | wip_msg <string 512>] | max_bandwidth_down [<int 0-536870911> | default] | max_bandwidth_up [<int 0-536870911> | default] | max_input_octets [<uint 0-4294967295> | default] | max_output_octets [<uint 0-4294967295> | default] | max_total_octets [<uint 0-4294967295> | default] | name [<name 32> | default] | protocol [http | https] | redirect [enable | disable] | redirect_url <string 255> | separator_color [<string 32> | default] | session_timeout [<int 0-86400> | default] | user_logout [enable | disable] | verification [guest | local | radius]]

show captive_portal configuration {<int 1-10> {[interface {[phy_port <portlist> | wireless_network <int 1-64>]} | status | locales | client]}}

config captive_portal client deauthenticate {[<int 1-10> | <macaddr>]}

show captive_portal client {<macaddr> {statistics}}

show captive_portal interface client {[phy_port <portlist> | wireless_network <int 1-64>]}

show captive_portal configuration client

show captive_portal interface configuration {<int 1-10>}

show captive_portal interface capability {[phy_port <portlist> | wireless_network <int 1-64>]}

create captive_portal user <int 1-128> [name <name 32> | password]

delete captive_portal user [all | <int 1-128>]

config captive_portal user <int 1-128> [group [add <int 1-10> | delete <int 1-10>] | idle_timeout [<int 0-900> | default] | max_bandwidth_down [<int 0-536870911> | default] | max_bandwidth_up [<int 0-536870911> | default] | max_input_octets [<uint 0-4294967295> | default] | max_output_octets [<uint 0-4294967295> | default] | max_total_octets [<uint 0-4294967295> | default] | name <name 32> | password {encrypted <password 128>} | session_timeout [<int 0-86400> | default]]

show captive_portal user {<int 1-128>}

create captive_portal user group <int 1-10>

delete captive_portal user group <int 1-10>

config captive_portal user group <int 1-10> [name <name 32> | moveusers <int 1-10>]

show captive_portal user group {<int 1-10>}

15-1 enable captive_portal

Description

This command is used to enable the Captive Portal operation on the Switch.

Format

enable captive_portal

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the Captive Portal:

```
DWS-3160-24PC:admin#enable captive_portal
Command: enable captive_portal

Success.

DWS-3160-24PC:admin#
```

15-2 disable captive_portal

Description

This command is used to disable the Captive Portal operation on the Switch.

Format

disable captive_portal

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the Captive Portal:

```
DWS-3160-24PC:admin#disable captive_portal
Command: disable captive_portal

Success.

DWS-3160-24PC:admin#
```

15-3 config captive_portal

Description

This command is used to configure the Captive Portal’s global settings on the Switch.

Format

config captive_portal [http_port [<int 0-65535> | default] | https_port [<int 0-65535> | default] | statistics_interval [0 | <int 15-3600> | default] | authentication_timeout [<int 60-600> | default]]

Parameters

http_port - Specifies to configure an additional HTTP port.
- **<int 0-65535>** - Enter the additional HTTP port value used here. This value must be between 0 and 65535. Ports 80 and 443 cannot be used as they are reserved. The default value is 0. The value 0 specifies that no additional HTTP port will be used.
- **default** - Specifies that the default value will be used.

https_port - Specifies to configure an additional HTTPS port.
- **<int 0-65535>** - Enter the additional HTTPS port value used here. This value must be between 0 and 65535. Ports 80 and 443 cannot be used as they are reserved. The default value is 0. The value 0 specifies that no additional HTTPS port will be used.
- **default** - Specifies that the default value will be used.

statistics_interval - Specifies the time interval, at which statistics are reported in the Cluster Controller, used.
- **0** - Specifies that statistics interval option will be disabled.
- **<int 15-3600>** - Enter the statistics interval value used here. This value must be between 15 and 3600 seconds. The default value is 120 seconds.
- **default** - Specifies that the default value will be used.

authentication_timeout - Specifies the time interval for authentication timeout.
- **<int 60-600>** - Enter the authentication timeout value used here. This value must be between 60 and 600 seconds. The default value is 300 seconds.
- **default** - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To configure the Captive Portal’s additional HTTP port:

```
DWS-3160-24PC:admin#config captive_portal http_port 100
Command: config captive_portal http_port 100

Success.

DWS-3160-24PC:admin#
```

To disable the Captive Portal’s statistics report option:

```
DWS-3160-24PC:admin#config captive_portal statistics_interval 0
Command: config captive_portal statistics_interval 0

Success.

DWS-3160-24PC:admin#
```

To configure the Captive Portal’s authentication timeout value:

```
DWS-3160-24PC:admin#config captive_portal authentication_timeout 600
Command: config captive_portal authentication_timeout 600

Success.

DWS-3160-24PC:admin#
```

15-4 config captive_portal trap

Description

This command is used to enable or disable Captive Portal SNMP traps.

Format

config captive_portal trap [enable | disable] [all | client_auth_failure | client_connect | client_disconnect | client_db_full]

Parameters

enable - Specifies that the Captive Portal trap option will be enabled.
disable - Specifies that the Captive Portal trap option will be disabled.

all - Specifies that all trap, concerning the Captive Portal, will be sent.
client_auth_failure - Specifies that a trap will be sent when a client attempts to authenticate with a Captive Portal but is unsuccessful.
client_connect - Specifies that a trap will be sent when a client authenticates with and connects to a Captive Portal.
client_disconnect - Specifies that a trap will be sent when a client disconnects from a Captive Portal.
client_db_full - Specifies that a trap will be sent each time an entry cannot be added to the client database because it is full.

Restrictions

Only Administrators can issue this command.

Example

To enable all Captive Portal SNMP traps:

```
DWS-3160-24PC:admin#config captive_portal trap enable all
Command: config captive_portal trap enable all

Success.

DWS-3160-24PC:admin#
```

To enable the Captive Portal SNMP trap option called ‘client-auth-failure’:

```
DWS-3160-24PC:admin#config captive_portal trap enable client_auth_failure
Command: config captive_portal trap enable client_auth_failure

Success.

DWS-3160-24PC:admin#
```

15-5 show captive_portal

Description

This command is used to display the Captive Portal’s global settings and status on the Switch.

Format

show captive_portal {[status | trap]}

Parameters

status - (Optional) Specifies to display the Captive Portal's global status.

trap - (Optional) Specifies to display the Captive Portal's SNMP trap configuration.

If no parameter is specified, then summarized information about the Captive Portal configuration will be displayed.

Restrictions

None.

Example

To display summarized information about the Captive Portal’s configuration when the Captive Portal is enabled:

```
DWS-3160-24PC:admin#show captive_portal
Command: show captive_portal

Administrative Mode                             : Enable
Operational Status                              : Enabled
CP IP Address                                   : 192.168.69.123

DWS-3160-24PC:admin#
```

To display summarized information about the Captive Portal's configuration when the Captive Portal is disabled:

```
DWS-3160-24PC:admin#show captive_portal
Command: show captive_portal

Administrative Mode                           : Disable
Operational Status                            : Disabled
Disable Reason                                : Administrator Disabled
CP IP Address                                 : 0.0.0.0

DWS-3160-24PC:admin#
```

To display the reporting status of all Captive Portal instances in the System:

```
DWS-3160-24PC:admin#show captive_portal status
Command: show captive_portal status

Additional HTTP Port                          : 100
Additional HTTP Secure Port                   : 0
Peer Switch Statistics Reporting Interval     : 0
Authentication Timeout                        : 600
Supported Captive Portals                     : 10
Configured Captive Portals                    : 1
Active Captive Portals                        : 0
Local Supported Users                         : 128
Configured Local Users                        : 0
System Supported Users                        : 1024
Authenticated Users                           : 0

DWS-3160-24PC:admin#
```

To display which Captive Portal SNMP traps are enabled:

```
DWS-3160-24PC:admin#show captive_portal trap
Command: show captive_portal trap

Client Authentication Failure Traps           : Enable
Client Connection Traps                       : Enable
Client Database Full Traps                    : Enable
Client Disconnection Traps                    : Enable

DWS-3160-24PC:admin#
```

In the above examples the following display parameters can be noticed:

Administrative Mode - Displays whether the CP is enabled or not.

Operational Status - Indicates whether the CP operational status is enabled or disabled.

Disable Reason - If the CP is disabled, this field displays the reason, which can be None, Administrator Disabled, IP Address Not Configured, No IP Routing Interface or Routing Disabled.

Captive Portal IP Address - Displays the IP address that the Captive Portal feature uses.

Additional HTTP Port - Displays the port number of the additional HTTP port configured for traffic. A value of 0 indicates that only port 80 is configured for HTTP traffic.

Additional HTTP Secure Port - Displays the port number of the additional HTTPS secure port. A value of 0 indicates no additional port and the default port (443) is used.

Peer Switch Statistics Reporting Interval - Displays the interval at which the peer switches send its authenticated client statistics to the Cluster Controller. The reporting interval is in the range of 0, 15-3600 seconds where 0 disables statistical reporting.

Authentication Timeout - Displays the number of seconds to keep the authentication session open with the client. When the timeout expires, the switch disconnects any active TCP or SSL connection with the client which means that if a CP user does not enter valid credentials within the time period, the authentication page will be served again in order for the client to gain access to the network.

Supported Captive Portals - Displays the number of supported Captive Portals in the system.

Configured Captive Portals - Displays the number of Captive Portals configured on the switch.

Active Captive Portals - Displays the number of Captive Portal instances that are operationally enabled.

Local Supported Users - Displays the number of users that can be added and configured using the local user database.

Configured Local Users - Displays the number of users that are configured from the local user database.

System Supported Users - Displays the total number of authenticated users that the system can support.

Authenticated Users - Displays the number of users currently authenticated to all Captive Portal instances on this switch.

Client Authentication Failure Traps - Displays whether the SNMP agent sends a trap when a client attempts to authenticate with a Captive Portal but is unsuccessful.

Client Connection Traps - Displays whether the SNMP agent sends a trap when a client authenticates with and connects to a Captive Portal.

Client Database Full Traps - Displays whether the SNMP agent sends a trap each time an entry cannot be added to the client database because it is full.

Client Disconnection Traps - Displays whether the SNMP agent sends a trap when a client disconnects from a Captive Portal.

15-6 create captive_portal configuration

Description

This command is used to create a Captive Portal configuration instance on the Switch.

Format

create captive_portal configuration <int 1-10>

Parameters

<int 1-10> - Enter the Captive Portal's configuration ID used here. This value must be between 1 and 10. The default value is 1.

Restrictions

Only Administrators can issue this command.

Example

To create a Captive Portal configuration ID:

```
DWS-3160-24PC:admin#create captive_portal configuration 2
Command: create captive_portal configuration 2

Success.

DWS-3160-24PC:admin#
```

15-7 delete captive_portal configuration

Description

This command is used to delete a Captive Portal configuration.

Format

delete captive_portal configuration <int 1-10>

Parameters

<int 1-10> - Enter the Captive Portal's configuration ID used here. This value must be between 1 and 10. The default value is 1 and cannot be deleted.

Restrictions

Only Administrators can issue this command.

Example

To delete a Captive Portal configuration ID:

```
DWS-3160-24PC:admin#delete captive_portal configuration 2
Command: delete captive_portal configuration 2

Success.

DWS-3160-24PC:admin#
```

15-8 config captive_portal configuration

Description

This command is used to configure the Captive Portal’s configurations on the Switch.

NOTE: Due to the complex nature of this command, it is advised to rather use the Web User Interface to customize the captive portal login page. For more information about this consult the Web UI Reference Guide.

Format

config captive_portal configuration <int 1-10>[background_color [<string 32> | default] | block [enable | disable] | clear | state [enable | disable] | foreground_color [<string 32> | default] | group [<int 1-10> | default] | idle_timeout [<int 0-900> | default] | interface [phy_port <portlist> | wireless_network <int 1-64>] [enable | disable] | locale <int 1-5> [accept_msg <string 512> | accept_text {<string 512>} | account_image <string 32> |

account_label {<string 256>} | aup_text {<string 32768>} | background_image <string 32> | branding_image <string 32> | browser_title {<string 512>} | button_label <string 128> | code <string 32> | denied_msg <string 512> | font_list {<sentence>} | instructional_text {<string 1024>} | link <string 512> | logout_browser_title {<string 512>} | logout_button_label <string 128> | logout_confirmation_text {<string 512>} | logout_success_background_image <string 32> | logout_success_browser_title {<string 512>} | logout_success_text {<string 1024>} | logout_success_title {<string 512>} | logout_text {<string 1024>} | logout_title {<string 512>} | password_label {<string 128>} | popup_text {<string 512>} | resource_msg <string 512> | script_text {<string 512>} | timeout_msg <string 512> | title_text {<string 512>} | user_label {<string 128>} | welcome_text {<string 1024>} | welcome_title {<string 512>} | wip_msg <string 512>] | max_bandwidth_down [<int 0-536870911> | default] | max_bandwidth_up [<int 0-536870911> | default] | max_input_octets [<uint 0-4294967295> | default] | max_output_octets [<uint 0-4294967295> | default] | max_total_octets [<uint 0-4294967295> | default] | name [<name 32> | default] | protocol [http | https] | redirect [enable | disable] | redirect_url <string 255> | separator_color [<string 32> | default] | session_timeout [<int 0-86400> | default] | user_logout [enable | disable] | verification [guest | local | radius]]

Parameters

<int 1-10> - Enter the Captive Portal configuration ID used here. This value must be between 1 and 10.

background_color - Specifies to customize the background color of the Captive Portal authentication page using a well-known color name or RGB value.
<string 32> - Enter the background color, of the Captive Portal authentication page, here. This string can be up to 32 characters long. This value must be a well-known color name or RGB value. The default value is #BFBFBF.
default - Specifies that the default value will be used.

block - Specifies to enable or disable the blocking of all traffic using the Captive Portal.
enable - Specifies that traffic blocking, using the Captive Portal, will be enabled.
disable - Specifies that traffic blocking, using the Captive Portal, will be disabled.

clear - Specifies to clear this instance to the default values.

state - Specifies to enables or disable the Captive Portal configuration.
enable - Specifies that the Captive Portal configuration will be enabled. This is the default option.
disable - Specifies that the Captive Portal configuration will be disabled.

foreground_color - Specifies to customize the foreground color of the Captive Portal authentication page using a well-known color name or RGB value.
<string 32> - Enter the foreground color, for the Captive Portal's authentication page, here. This string can be up to 32 characters long. The default value is #999999
default - Specifies that the default value will be used.

group - Specifies to assign a group ID to a Captive Portal configuration. Each Captive Portal configuration must contain at least one group ID.
<int 1-10> - Enter the group ID value, linked to a Captive Portal configuration, here. This value must be between 1 and 10. The default value is 1.
default - Specifies that the default value will be used.

idle_timeout - Specifies the idle timeout value for a Captive Portal configuration.
<int 0-900> - Enter the idle timeout value, for a Captive Portal configuration, here. This value must be between 0 and 900 seconds. The value of 0 will disable to option. The default value is 0.
default - Specifies that the default value will be used.

interface - Specifies to associate an interface to a Captive Portal configuration or to remove the interface Captive Portal association. The interface can be physical ports or wireless networks.
phy_port - Specifies the physical ports used.
<portlist> - Enter the physical port number(s) used here.
wireless_network - Specifies the wireless network used.

<int 1-64> - Enter the wireless network value used here. This value must be between 1 and 64.

enable - Specifies that the interface association option will be enabled.

disable - Specifies that the interface association option will be disabled.

locale - Specifies that the administrator must use the WEB user interface to create and customize Captive Portal web content. The command is primarily used by the Switch's 'show running config command' and process as it provides the ability to save and restore configurations using a text-based format.

<int 1-5> - Enter the locale value used here. This value must be between 1 and 5.

accept_msg - Specifies that the web user must enter the text to display when the user did not accept the usage acceptance policy. This message displays after the user clicks the button to connect to the network.

<string 512> - Enter the acceptance message, to be displayed, here. This message can be up to 512 characters long.

accept_text - Specifies that the web user must enter the text to display next to the box that the user must select to indicate that he or she accepts the terms of use.

<string 512> - (Optional) Enter the acceptance text, to be displayed, here. This text can be up to 512 characters long.

account_image - Specifies that the web user must select the image that will be displayed on the Captive Portal page above the login field.

<string 32> - Enter the account image name used here. This name can be up to 32 characters long.

account_label - Specifies that the web user must enter the summary text to display that instructs users to authenticate.

<string 256> - (Optional) Enter the account label string used here. This string can be up to 256 characters long.

aup_text - Specifies that the web user must enter the text to display in the Acceptance Use Policy field. The acceptance use policy instructs users about the conditions under which they are allowed to access the network.

<string 32768> - (Optional) Enter the Acceptance Use Policy text here. This text can be up to 32768 characters long.

background_image - Specifies that the web user must select the name of the image to display as the page background.

<string 32> - Enter the background image name used here. This name can be up to 32 characters long.

branding_image - Specifies that the web user must select the name of the image file to display on the top left corner of the page. This image is used for branding purposes, such as the company logo.

<string 32> - Enter the branding image name used here. This name can be up to 32 characters long.

browser_title - Specifies that the web user must enter the text to display on the client's Web browser title bar or tab.

<string 512> - (Optional) Enter the browser title string used here. This string can be up to 512 characters long.

button_label - Specifies that the web user must enter the button label text used.

<string 128> - Enter the button label text used here. This label can be up to 128 characters long.

code - Specifies that the web user must enter the Language code for the language.

<string 32> - Enter the language code string used here. This string can be up to 32 characters long.

denied_msg - Specifies that the web user must enter the text to display when the user does not provide valid authentication information.

<string 512> - Enter the denied message string used here. This string can be up to 512 characters long.

font_list - Specifies that the web user must enter the name of the font to use for all the text on the Captive Portal page.

<sentence> - (Optional) Enter the font list name used here.

instructional_text - Specifies that the web user must enter the detailed text to display that instructs users to authenticate.

<string 1024> - (Optional) Enter the instructional authentication text used here. This string can be up to 1024 characters long.

link - Specifies that the web user must add a Captive Portal configuration in a language that is supported by the Switch.

<string 512> - Enter the Captive Portal link string used here. This string must be up to 512 characters long.

logout_browser_title - Specifies that the web user must enter the text to display on the title bar of the Logout page.

<string 512> - (Optional) Enter the Logout browser title string used here. This string can be up to 512 characters long.

logout_button_label - Specifies that the web user must enter the text to display on the button the user clicks to deauthenticate.

<string 128> - Enter the Logout button label text here. This string can be up to 128 characters long.

logout_confirmation_text - Specifies that the web user must enter a more detailed text display that prompts users to confirm the de-authentication process.

<string 512> - (Optional) Enter the Logout confirmation text used here. This string can be up to 512 characters long.

logout_success_background_image - Specifies that the web user must enter the name of the current background image on the Logout Success page.

<string 32> - Enter the Logout success background image name used here. This name can be up to 32 characters long.

logout_success_browser_title - Specifies that the web user must enter the text to display on the title bar of the Logout Success page.

<string 512> - (Optional) Enter the Logout success browser title string used here. This string can be up to 512 characters long.

logout_success_text - Specifies that the web user must enter the text to display that confirms that the user has been deauthenticated.

<string 1024> - (Optional) Enter the Logout success message used here. This string can be up to 1024 characters long.

logout_success_title - Specifies that the web user must enter the text used as the page title. This is the text that identifies the page.

<string 512> - (Optional) Enter the Logout success title string here. This string can be up to 512 characters long.

logout_text - Specifies that the web user must enter a more detailed text display that confirms that the user has been authenticated and instructs the user on how to deauthenticate.

<string 1024> - (Optional) Enter the Logout text used here. This string can be up to 1024 characters long.

logout_title - Specifies that the web user must enter the text that will be used as the page title. This is the text that identifies the page.

<string 512> - (Optional) Enter the Logout title string used here. This string can be up to 512 characters long.

password_label - Specifies that the web user must enter the text that will be displayed next to the field where the user enters the password.

<string 128> - (Optional) Enter the password label used here. This string can be up to 128 characters long.

popup_text - Specifies that the web user must Specifies the text to indicate that users must allow pop-up windows to display the logout WEB page. This field is only applicable when the user logout mode is enabled. You can modify this text whether the feature is enabled or disabled.

<string 512> - (Optional) Enter the pop-up logout text used here. This string can be up to 512 characters long.

resource_msg - Specifies that the web user must enter the text to display when the system has rejected authentication due to system resource limitations. This message displays after the user clicks the button to connect to the network.

<string 512> - Enter the resource message, to be displayed, here. This string can be up to 512 characters long.

script_text - Specifies that the web user must Specifies the text to indicate that users must enable JavaScript to display the logout WEB page. This field is only applicable when the user logout mode is enabled. You can modify the text whether the feature is enabled or disabled.

<string 512> - (Optional) Enter the JavaScript logout message, to be displayed here. This string can be up to 512 characters long.

timeout_msg - Specifies that the web user must enter the text that will be displayed when the system has rejected authentication because the authentication transaction took too long. This could be due to the user's input time, or a timeout due to the overall transaction.

<string 512> - Enter the timeout message used here. This string can be up to 512 characters long.

title_text - Specifies that the web user must enter the text to use as the page title. This is the text that identifies the page.

<string 512> - (Optional) Enter the page title text used here. This string can be up to 512 characters long.

user_label - Specifies that the web user must enter the text that will be displayed next to the field where the user enters the username.

<string 128> - (Optional) Enter the user label used here. This string can be up to 128 characters long.

welcome_text - Specifies that the web user must enter the text that will be displayed to further identify the network that will be accessed by the Captive Portal user. This message displays under the Welcome Title.

<string 1024> - (Optional) Enter the more descriptive welcome text used here. This string can be up to 1024 characters long.

welcome_title - Specifies that the web user must enter the title that will be displayed, to greet the user, after successfully connecting to the network.

<string 512> - (Optional) Enter the welcome title used here. This string can be up to 512 characters long.

wip_msg - Specifies that the web user must enter the text to display when the validation is in progress. This message displays after the user clicks the button to connect to the network.

<string 512> - Enter the authentication failure error message, that will be displayed, here. This string can be up to 512 characters long.

max_bandwidth_down - Specifies the maximum rate, at which a client can receive data from the network.

<int 0-536870911> - Enter the maximum down bandwidth value used here. This value must be between 0 and 536870911 bits per second. The value 0 indicates that there will be no limit. The default value is 0.

default - Specifies that the default value will be used.

max_bandwidth_up - Specifies the maximum rate at which a client can send data into the network.

<int 0-536870911> - Enter the maximum up bandwidth value used here. This value must be between 0 and 536870911 bits per second. The value 0 indicates that there will be no limit. The default value is 0.

default - Specifies that the default value will be used.

max_input_octets - Specifies the maximum number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected.

<uint 0-4294967295> - Enter the maximum input octets value used here. This value must be between 0 and 4294967295. The value 0 indicates that there will be no limit. The default value is 0.

default - Specifies that the default value will be used.

max_output_octets - Specifies the maximum number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected.

<uint 0-4294967295> - Enter the maximum output octets value used here. This value must be between 0 and 4294967295. The value 0 indicates that there will be no limit. The default value is 0.

default - Specifies that the default value will be used.

max_total_octets - Specifies the maximum number of octets the user is allowed to transfer. The sum of octets transmitted and received. After this limit has been reached the user will be disconnected.

<uint 0-4294967295> - Enter the maximum total octets value used here. This value must be between 0 and 4294967295. The value 0 indicates that there will be no limit. The default value is 0.

default - Specifies that the default value will be used.

name - Specifies the name for the Captive Portal configuration.

- **<name 32>** - Enter the Captive Portal configuration name used here. This name can be up to 32 characters long.
- **default** - Specifies that the default value will be used.

protocol - Specifies the protocol used for the Captive Portal configuration. The Captive Portal can use either HTTP or HTTPS protocols.

- **http** - Specifies that the protocol used, for the Captive Portal configuration, is HTTP. This is the default option.
- **https** - Specifies that the protocol used, for the Captive Portal configuration, is HTTPS.

redirect - Specifies to enable or disable the redirect mode for the Captive Portal configuration.

- **enable** - Specifies that the redirect mode, for the Captive Portal configuration, will be enabled.
- **disable** - Specifies that the redirect mode, for the Captive Portal configuration, will be disabled. This is the default option.

redirect_url - Specifies the URL that the newly authenticated client will be redirected to, if the URL Redirect Mode is enabled.

- **<string 255>** - Enter the redirect URL string used here. This string can be up to 255 characters long.

separator_color - Specifies to customize the separator bar color of the Captive Portal authentication page.

- **<string 32>** - Enter the separator bar's color value used here. This value can be up to 32 characters long. The default value is #326BA0.
- **default** - Specifies that the default value will be used.

session_timeout - Specifies the session timeout for the Captive Portal configuration.

- **<int 0-86400>** - Enter the session timeout value used here. This value must be between 0 and 86400 seconds. The value of 0, indicates that no timeout will be enforced. The default value is 86400.
- **default** - Specifies that the default value will be used.

user_logout - Specifies to enable or disable the ability for an authenticated user to de-authenticate from the network.

- **enable** - Specifies that an authenticated user will have the ability to de-authenticate from the network.
- **disable** - Specifies that an authenticated user will not have the ability to de-authenticate from the network.

verification - Specifies the verification mode for a Captive Portal configuration.

- **guest** - Specifies that the user does not need to be authenticated using a database. This is the default option.
- **local** - Specifies that the Switch will use the local database to authenticate users.
- **radius** - Specifies that the Switch will use a database on a remote RADIUS server to authenticate users.

Restrictions

Only Administrators can issue this command.

Example

To disable the Captive Portal configuration 1:

```
DWS-3160-24PC:admin#config captive_portal configuration 1 state disable
Command: config captive_portal configuration 1 state disable

Success.

DWS-3160-24PC:admin#
```

To configure the Captive Portal configuration to the default values:

```
DWS-3160-24PC:admin#config captive_portal configuration 1 clear
Command: config captive_portal configuration 1 clear

All fields will be set to the default values for this CP configuration.
Are you sure you want to clear the CP configuration? (y/n) y
Success.

DWS-3160-24PC:admin#
```

To enable traffic blocking on the Captive Portal configuration 1:

```
DWS-3160-24PC:admin#config captive_portal configuration 1 block enable
Command: config captive_portal configuration 1 block enable

Success.

DWS-3160-24PC:admin#
```

To customize the background color of the Captive Portal authentication page:

```
DWS-3160-24PC:admin#config captive_portal configuration 1 background_color
#FFFFFF
Command: config captive_portal configuration 1 background_color #FFFFFF

Success.

DWS-3160-24PC:admin#
```

To configure the session timeout value for the Captive Portal configuration:

```
DWS-3160-24PC:admin#config captive_portal configuration 1 session_timeout 1200
Command: config captive_portal configuration 1 session_timeout 1200

Success.

DWS-3160-24PC:admin#
```

To configure the verification mode for the Captive Portal configuration:

```
DWS-3160-24PC:admin#config captive_portal configuration 1 verification local
Command: config captive_portal configuration 1 verification local

Success.

DWS-3160-24PC:admin#
```

To enable the user logout option for the Captive Portal configuration:

```
DWS-3160-24PC:admin#config captive_portal configuration 1 user_logout enable
Command: config captive_portal configuration 1 user_logout enable

Success.

DWS-3160-24PC:admin#
```

To enable the redirect mode option for the Captive Portal configuration:

```
DWS-3160-24PC:admin#config captive_portal configuration 1 redirect enable
Command: config captive_portal configuration 1 redirect enable

Success.

DWS-3160-24PC:admin#
```

To configure a redirect URL for the Captive Portal configuration:

```
DWS-3160-24PC:admin#config captive_portal configuration 1 redirect_url
http://www.company.com
Command: config captive_portal configuration 1 redirect_url
http://www.company.com

Success.

DWS-3160-24PC:admin#
```

To configure the name for the Captive Portal configuration:

```
DWS-3160-24PC:admin#config captive_portal configuration 1 name Training
Command: config captive_portal configuration 1 name Training

Success.

DWS-3160-24PC:admin#
```

To configure the protocol for the Captive Portal configuration:

```
DWS-3160-24PC:admin#config captive_portal configuration 1 protocol https
Command: config captive_portal configuration 1 protocol https

Success.

DWS-3160-24PC:admin#
```

To configure the group for the Captive Portal configuration:

```
DWS-3160-24PC:admin#config captive_portal configuration 1 group 2
Command: config captive_portal configuration 1 group 2

Success.

DWS-3160-24PC:admin#
```

To configure the maximum rate at which a client can receive data from the network for the Captive Portal configuration:

```
DWS-3160-24PC:admin#config captive_portal configuration 1 max_bandwidth_down
102400
Command: config captive_portal configuration 1 max_bandwidth_down 102400

Success.

DWS-3160-24PC:admin#
```

To associate a wireless network interface 10 to the Captive Portal configuration 1:

```
DWS-3160-24PC:admin#config captive_portal configuration 1 interface
wireless_network 10 enable
Command: config captive_portal configuration 1 interface wireless_network 10
enable

Success.

DWS-3160-24PC:admin#
```

15-9 show captive_portal configuration

Description

This command is used to display the Captive Portal configuration on the Switch.

Format

show captive_portal configuration {<int 1-10> {[interface {[phy_port <portlist> | wireless_network <int 1-64>]} | status | locales | client]}}

Parameters

<int 1-10> - (Optional) Enter the Captive Portal configuration instance ID here. This value must be between 1 and 10. If this variable is not specified, then this command will display information of all the configured Captive Portal configurations.

interface - (Optional) Specifies to display all interfaces assigned to the Captive Portal configuration.

- **phy_port** - Specifies to display information for interfaces of the specified physical port(s) assigned to the Captive Portal configuration.
  - **<portlist>** - Enter the physical portlist used here.
- **wireless_network** - Specifies to display information for interfaces of a wireless network assigned to the Captive Portal configuration.
  - **<int 1-64>** - Enter the wireless network ID used here. This value must be between 1 and 64.

status - (Optional) Specifies to display status information of a specific Captive Portal configuration.

locales - (Optional) Specifies to display locales associated with the specific Captive Portal configuration.

client - (Optional) Specifies to display the clients authenticated to a specific configuration.

Restrictions

None.

Example

To display information of all configured Captive Portal configurations:

```
DWS-3160-24PC:admin#show captive_portal configuration
Command: show captive_portal configuration

CP ID       CP Name         Mode   Protocol Verification
----- ------------------- ------- -------- ------------
1     Training            Enable  HTTPS    Local

Total Entries : 1

DWS-3160-24PC:admin#
```

To display information of a specific Captive Portal configuration:

```
DWS-3160-24PC:admin#show captive_portal configuration 1
Command: show captive_portal configuration 1

CP ID                                         : 1
CP Name                                       : Training
Operational Status                            : Enabled
Block Status                                  : Blocked
Configured Locales                            : 1
Authenticated Users                           : 0

DWS-3160-24PC:admin#
```

To display all the interfaces assigned to the Captive Portal configuration 1:

```
DWS-3160-24PC:admin#show captive_portal configuration 1 interface
Command: show captive_portal configuration 1 interface

CP ID                                         : 1
CP Name                                       : Training

                                          Activation    Block
       Interface Description                Status      Status
---------------------------------------- ------------ -----------
Wireless Network 10 - dlink10            Enabled      Blocked

Total Entries : 1

DWS-3160-24PC:admin#
```

To display the status of the physical port 2 for the Captive Portal configuration 1:

```
DWS-3160-24PC:admin#show captive_portal configuration 1 interface phy_port 2
Command: show captive_portal configuration 1 interface phy_port 2

CP ID                                         : 1
CP Name                                       : Training
Interface                                     : Physical Port 2
Interface Description                         : Physical Port: 2 Gigabit - L...
Activation Status                             : Enabled
Block Status                                  : Not Blocked
Authenticated Users                           : 0

Total Entries : 0

DWS-3160-24PC:admin#
```

To display the status of the wireless interface 1 for the Captive Portal configuration 1:

```
DWS-3160-24PC:admin#show captive_portal configuration 1 interface
wireless_network 10
Command: show captive_portal configuration 1 interface wireless_network 10

CP ID                                         : 1
CP Name                                       : Training
Interface                                     : Wireless Network 10
Interface Description                         : Wireless Network 10 - dlink10
Activation Status                             : Enabled
Block Status                                  : Blocked
Authenticated Users                           : 0

Total Entries : 0

DWS-3160-24PC:admin#
```

To display the status of the Captive Portal configuration 1:

```
DWS-3160-24PC:admin#show captive_portal configuration 1 status
Command: show captive_portal configuration 1 status

CP ID                                          : 1
CP Name                                        : Training
CP Mode                                        : Enable
Protocol Mode                                  : HTTPS
Verification Mode                              : Local
Group ID                                       : 2
Group Name                                     :
User Logout Mode                               : Enable
URL Redirect Mode                              : Enable
Redirect URL                                   : http://www.company.com
Session Timeout                                : 1200
Idle Timeout                                   : 0
Max Bandwidth Up (bytes/sec)                   : 0
Max Bandwidth Down (bytes/sec)                 : 102400
Max Input Octets (bytes)                       : 0
Max Output Octets (bytes)                      : 0
Max Total Octets (bytes)                       : 0

DWS-3160-24PC:admin#
```

To display the locales for the Captive Portal configuration 1:

```
DWS-3160-24PC:admin#show captive_portal configuration 1 locales
Command: show captive_portal configuration 1 locales

Locale Code
---------------
en

DWS-3160-24PC:admin#
```

To display the client's status which authenticated to the Captive Portal configuration 1:

```
DWS-3160-24PC:admin#show captive_portal configuration 1 client
Command: show captive_portal configuration 1 client

CP ID                                          : 1
CP Name                                        : Training

No Captive Portal clients exist.

DWS-3160-24PC:admin#
```

In the above examples the following display parameters can be noticed:

CP ID - Displays the Captive Portal ID.

CP Name - Displays the Captive Portal name.

Operational Status - Displays whether the Captive Portal is enabled or disabled.

Disable Reason - If the Captive Portal is disabled, this field indicates the reason.

Blocked Status - Displays the blocked status, which is Blocked or Not Blocked.

Authenticated Users - Displays the number of authenticated users connected to the network through this Captive Portal.

Configured Locales - Displays the number of locales defined for this Captive Portal.

Interface Description - Describes the interface.

Block Status - Displays the blocked status, which is Blocked or Not Blocked.

Disable Reason - If the Captive Portal is disabled, this field indicates the reason.

CP Mode - Displays whether the CP is enabled or disabled.

Protocol Mode - Displays the current connection protocol, which is either HTTP or HTTPS.

Verification Mode - Displays the current account type, which is Guest, Local, or RADIUS.

URL Redirect Mode - Displays whether the Redirect URL Mode is enabled or disabled.

Max Bandwidth Up (bytes/sec) - Displays the maximum rate in bytes per second (Bps) at which a client can send data into the network.

Max Bandwidth Down (bytes/sec) - Displays the maximum rate in bytes per second (Bps) at which a client can receive data from the network.

Max Input Octets (bytes) - Displays the maximum number of octets a client is allowed to receive.

Max Output Octets (bytes) - Displays the maximum number of octets a client is allowed to transmit.

Max Total Octets (bytes) - Displays the maximum number of octets a client is allowed to transfer, i.e., the sum of octets transmitted and received.

Session Timeout (seconds) - Displays the number of seconds a user is permitted to remain connected to the network. Once the Session Timeout value is reached, the user is logged out automatically. A value of 0 means that the user does not have a session timeout limit.

Idle Timeout (seconds) - Displays the number of seconds the user can remain idle before the switch automatically logs the user out. A value of 0 means that the user will not be logged out automatically.

Locale Code - Displays the two-letter abbreviation for languages.

15-10 config captive_portal client deauthenticate

Description

This command is used to deauthenticate a specific Captive Portal client or all Captive Portal clients.

Format

config captive_portal client deauthenticate {[<int 1-10> | <macaddr>]}

Parameters

<int 1-10> - (Optional) Enter a Captive Portal configuration ID, used to indicate the Captive Portal configuration that the client is de-authenticating from, here. This value must be between 1 and 10.

<macaddr> - (Optional) Enter the MAC address of the client to deauthenticate here.

If no parameter is specified, then all clients will be deauthenticated from the Captive Portal.

Restrictions

Only Administrators can issue this command.

Example

To deauthenticate all Captive Portal clients:

```
DWS-3160-24PC:admin#config captive_portal client deauthenticate
Command: config captive_portal client deauthenticate

Successfully deauthenticated clients.

Success.

DWS-3160-24PC:admin#
```

To deauthenticate all Captive Portal clients from Configuration 1:

```
DWS-3160-24PC:admin#config captive_portal client deauthenticate 1
Command: config captive_portal client deauthenticate 1

Successfully deauthenticated clients for CP configuration 1.

Success.

DWS-3160-24PC:admin#
```

To deauthenticate a specific Captive Portal client:

```
DWS-3160-24PC:admin#config captive_portal client deauthenticate 00-23-7D-BC-2E-
18
Command: config captive_portal client deauthenticate 00-23-7D-BC-2E-18

Are you sure you want to deauthenticate the client? (y/n) y
CP client deauthenticated.

Success.

DWS-3160-24PC:admin#
```

15-11 show captive_portal client

Description

This command is used to display information about the clients connected to the Captive Portals configured on the Switch.

Format

show captive_portal client {<macaddr> {statistics}}

Parameters

<macaddr> - (Optional) Enter the MAC address of the wireless client here.

statistics - (Optional) Specifies to display the statistics for a specific Captive Portal client.

If no parameter is specified, then a summary of the Captive Portal client connection will be displayed.

Restrictions

None.

Example

To display the Captive Portal client connection summary:

```
DWS-3160-24PC:admin#show captive_portal client
Command: show captive_portal client

      MAC Address                                        Verify
(*)Peer Authenticated   IP Address    User Name  Protocol  Mode  Session Time
--------------------- --------------- ---------- -------- ------ ------------
 00-23-7D-BC-2E-18    192.168.69.66   localuser  HTTP      Guest  0d:00:00:07

Total Entries : 1

DWS-3160-24PC:admin#
```

To display the client connection details for a specific connected Captive Portal user:

```
DWS-3160-24PC:admin#show captive_portal client 00-23-7D-BC-2E-18
Command: show captive_portal client 00-23-7D-BC-2E-18

Client MAC Address                              : 00-23-7D-BC-2E-18
Client IP Address                               : 192.168.69.66
Protocol Mode                                   : HTTP
Verification Mode                               : Guest
CP ID                                           : 1
CP Name                                         : Default
Interface                                       : Physical Port 23
Interface Description                           : Physical Port: 23 Gigabit -
L...
User Name                                       : localuser
Session Time                                    : 0d:00:00:31
Switch MAC Address                              : 00-11-22-33-45-67
Switch IP Address                               : 192.168.69.123
Switch Type                                     : Local

DWS-3160-24PC:admin#
```

To display the client connection statistics for a specific Captive Portal user:

```
DWS-3160-24PC:admin#show captive_portal client 00-23-7D-BC-2E-18 statistics
Command: show captive_portal client 00-23-7D-BC-2E-18 statistics

Client MAC Address                              : 00-23-7D-BC-2E-18
Bytes Received                                  : 0
Bytes Transmitted                               : 0
Packets Received                                : 0
Packets Transmitted                             : 0

DWS-3160-24PC:admin#
```

In the above examples the following display parameters can be noticed:

Client MAC Address - Displays the MAC address of the wireless or wired client.

Client IP Address - Displays the IP address of the wireless or wired client.

Protocol Mode - Displays the current connection protocol, which is either HTTP or HTTPS.

Verification Mode - Displays the current account type, which is Guest, Local, or RADIUS.

Session Time - Displays the amount of time that has passed since the client was authorized.

CP ID - Displays the Captive Portal ID the connected client is using.

CP Name - Displays the name of the Captive Portal the connected client is using.

Interface - Displays the interface can be physical ports or wireless networks.

Interface Description - Displays the interface.

User Name - Displays the user name (or Guest ID) of the connected client.

Switch MAC Address - Displays the MAC address of the switch.

Switch IP Address - Displays the IP address of the switch.

Switch Type (local or peer) - Displays the current switch type, which is local or peer.

Bytes Received - Displays the total bytes the client has received.

Bytes Transmitted - Displays the total bytes the client has transmitted.

Packets Transmitted - Displays the total packets the client has transmitted.

Packets Received - Displays the total packets the client has received.

15-12 show captive_portal interface client

Description

This command is used to display information about clients authenticated on all interfaces or a specific interface.

Format

show captive_portal interface client {[phy_port <portlist> | wireless_network <int 1-64>]}

Parameters

phy_port - (Optional) Specifies to display client information on the physical port(s).
  <portlist> - Enter the physical portlist used here.

wireless_network - (Optional) Specifies to display client information on the wireless network.
  <int 1-64> - Enter the wireless network ID used here.

Restrictions

None.

Example

To display a summary of all interfaces for connected Captive Portal users:

```
DWS-3160-24PC:admin#show captive_portal interface client
Command: show captive_portal interface client

                                        Client          Client
      Interface Description           MAC Address      IP Address
----------------------------------- ----------------- ---------------
Physical Port: 1 Gigabit - Level
Physical Port: 2 Gigabit - Level
Physical Port: 3 Gigabit - Level
Physical Port: 4 Gigabit - Level
Physical Port: 5 Gigabit - Level
Physical Port: 6 Gigabit - Level
Physical Port: 7 Gigabit - Level
Physical Port: 8 Gigabit - Level
Physical Port: 9 Gigabit - Level
Physical Port: 10 Gigabit - Level
Physical Port: 11 Gigabit - Level
Physical Port: 12 Gigabit - Level
Physical Port: 13 Gigabit - Level
Physical Port: 14 Gigabit - Level
Physical Port: 15 Gigabit - Level
Physical Port: 16 Gigabit - Level
Physical Port: 17 Gigabit - Level
Physical Port: 18 Gigabit - Level
Physical Port: 19 Gigabit - Level
Physical Port: 20 Gigabit - Level
Physical Port: 21 Gigabit - Level
Physical Port: 22 Gigabit - Level
Physical Port: 23 Gigabit - Level   00-23-7D-BC-2E-18 192.168.69.66
Physical Port: 24 Gigabit - Level
Wireless Network 1 - dlink1
Wireless Network 2 - dlink2
Wireless Network 3 - dlink3
Wireless Network 4 - dlink4
Wireless Network 5 - dlink5
Wireless Network 6 - dlink6
Wireless Network 7 - dlink7
Wireless Network 8 - dlink8
Wireless Network 9 - dlink9
Wireless Network 10 - dlink10
Wireless Network 11 - dlink11
Wireless Network 12 - dlink12
Wireless Network 13 - dlink13
Wireless Network 14 - dlink14
Wireless Network 15 - dlink15
Wireless Network 16 - dlink16

Total Entries : 1

DWS-3160-24PC:admin#
```

To display detailed information for Captive Portal users connected to a specific interface:

```
DWS-3160-24PC:admin#show captive_portal interface client phy_port 23
Command: show captive_portal interface client phy_port 23

Interface             : Physical Port 23
Interface Description : Physical Port: 23 Gigabit - L...

     Client           Client
   MAC Address      IP Address    CP ID      CP Name      Protocol Verification
----------------- --------------  ----- ----------------- -------- ------------
00-23-7D-BC-2E-18 192.168.69.66   1     Default           HTTP     Guest
Total Entries : 1

DWS-3160-24PC:admin#
```

15-13 show captive_portal configuration client

Description

This command is used to display the clients authenticated to all Captive Portal configurations on the Switch.

Format

show captive_portal configuration client

Parameters

None.

Restrictions

None.

Example

To display the clients authenticated to all Captive Portal configurations on the Switch:

```
DWS-3160-24PC:admin#show captive_portal configuration client
Command: show captive_portal configuration client

CP ID      CP Name            Client            Client          Interface
                            MAC Address       IP Address
----- ----------------- ------------------ --------------- --------------------
1     Default           00-23-7D-BC-2E-18  192.168.69.66   Physical Port 23

Total Entries : 1

DWS-3160-24PC:admin#
```

15-14 show captive_portal interface configuration

Description

This command is used to display the interface configuration assignments for all Captive Portal configurations or a specific configuration.

Format

show captive_portal interface configuration {<int 1-10>}

Parameters

<int 1-10> - (Optional) Enter the Captive Portal configuration ID used here. If this variable is not specified, all Captive Portal configurations are displayed.

Restrictions

None.

Example

To display the interface configuration assignments for all Captive Portal configurations:

```
DWS-3160-24PC:admin#show captive_portal interface configuration
Command: show captive_portal interface configuration

CP ID      CP Name              Interface Description          Type
----- ------------------ ----------------------------------- --------
1     Default            Physical Port: 23 Gigabit - Level   Physical

DWS-3160-24PC:admin#
```

To display the interface configuration assignments for a specific Captive Portal configuration:

```
DWS-3160-24PC:admin#show captive_portal interface configuration 1
Command: show captive_portal interface configuration 1

CP ID                                         : 1
CP Name                                       : Default

       Interface Description          Type
----------------------------------- --------
Physical Port: 23 Gigabit - Level   Physical

Total Interfaces: 1

DWS-3160-24PC:admin#
```

15-15 show captive_portal interface capability

Description

This command is used to display all the Captive Portal eligible interfaces or the interface capabilities for a specific Captive Portal interface.

Format

show captive_portal interface capability {[phy_port <portlist> | wireless_network <int 1-64>]}

Parameters

phy_port - (Optional) Specifies to display the client information on the physical port(s).
<portlist> - Enter the physical portlist used here.

wireless_network - (Optional) Specifies to display the client information on the wireless network.
<int 1-64> - Enter the wireless network ID used here.

Restrictions

None.

Example

To display all capable Captive Portal interfaces:

```
DWS-3160-24PC:admin#show captive_portal interface capability
Command: show captive_portal interface capability

      Interface Description                Type
---------------------------------------- ----------
Physical Port: 1 Gigabit - Level         Physical
Physical Port: 2 Gigabit - Level         Physical
Physical Port: 3 Gigabit - Level         Physical
Physical Port: 4 Gigabit - Level         Physical
Physical Port: 5 Gigabit - Level         Physical
Physical Port: 6 Gigabit - Level         Physical
Physical Port: 7 Gigabit - Level         Physical
Physical Port: 8 Gigabit - Level         Physical
Physical Port: 9 Gigabit - Level         Physical
Physical Port: 10 Gigabit - Level        Physical
Physical Port: 11 Gigabit - Level        Physical
Physical Port: 12 Gigabit - Level        Physical
Physical Port: 13 Gigabit - Level        Physical
Physical Port: 14 Gigabit - Level        Physical
Physical Port: 15 Gigabit - Level        Physical
Physical Port: 16 Gigabit - Level        Physical
Physical Port: 17 Gigabit - Level        Physical
Physical Port: 18 Gigabit - Level        Physical
Physical Port: 19 Gigabit - Level        Physical
Physical Port: 20 Gigabit - Level        Physical
Physical Port: 21 Gigabit - Level        Physical
Physical Port: 22 Gigabit - Level        Physical
Physical Port: 23 Gigabit - Level        Physical
Physical Port: 24 Gigabit - Level        Physical
Wireless Network 1 - dlink1              Wireless
Wireless Network 2 - dlink2              Wireless
Wireless Network 3 - dlink3              Wireless
Wireless Network 4 - dlink4              Wireless
Wireless Network 5 - dlink5             Wireless
Wireless Network 6 - dlink6             Wireless
Wireless Network 7 - dlink7             Wireless
Wireless Network 8 - dlink8             Wireless
Wireless Network 9 - dlink9             Wireless
Wireless Network 10 - dlink10           Wireless
Wireless Network 11 - dlink11           Wireless
Wireless Network 12 - dlink12           Wireless
Wireless Network 13 - dlink13           Wireless
Wireless Network 14 - dlink14           Wireless
Wireless Network 15 - dlink15           Wireless
Wireless Network 16 - dlink16           Wireless

Total Interfaces: 40

DWS-3160-24PC:admin#
```

To display the specific capable interface:

```
DWS-3160-24PC:admin#show captive_portal interface capability wireless_network 1
Command: show captive_portal interface capability wireless_network 1

Interface                                    : Wireless Network 1
Interface Description                        : Wireless Network 1 - dlink1
Interface Type                               : Wireless
Session Timeout                              : Supported
Idle Timeout                                 : Supported
Bytes Received Counter                       : Supported
Bytes Transmitted Counter                    : Supported
Packets Received Counter                     : Supported
Packets Transmitted Counter                  : Supported
Roaming                                      : Supported

DWS-3160-24PC:admin#
```

In the above examples the following display parameters can be noticed:

Interface Description - Displays the interface description.

Interface Type - Displays the type of interface.

Session Timeout - Displays whether or not this field is supported by the specified Captive Portal interface.

Idle Timeout - Displays whether or not this field is supported by the specified Captive Portal interface.

Bytes Received Counter - Displays whether or not this field is supported by the specified Captive Portal interface.

Bytes Transmitted Counter - Displays whether or not this field is supported by the specified Captive Portal interface.

Packets Received Counter - Displays whether or not this field is supported by the specified Captive Portal interface.

Packets Transmitted Counter - Displays whether or not this field is supported by the specified Captive Portal interface.

Roaming - Displays whether or not this field is supported by the specified Captive Portal interface.

15-16 create captive_portal user

Description

This command is used to create a captive portal user in the local database. There are two ways to create the user. Create using a name or create using a password. If the user is created using name, the password needs to be assigned with the user password command. If the user is created using password, the name can be assigned later.

Format

create captive_portal user <int 1-128> [name <name 32> | password]

Parameters

<int 1-128> - Enter the User ID used here. This value must be between 1 and 128.

name - Specifies the name of the user ID. This name is used at the client station for authentication.
<name 32> - Enter the user's name used here. This name can be up to 32 characters long.

password - Specifies the user ID’s password.

Restrictions

Only Administrators can issue this command.

Example

To create a user using a name:

```
DWS-3160-24PC:admin#create captive_portal user 2 name newuser
Command: create captive_portal user 2 name newuser

Success.

DWS-3160-24PC:admin#
```

To create a user using the password:

```
DWS-3160-24PC:admin#create captive_portal user 3 password
Command: create captive_portal user 3 password

 Enter a case-sensitive new password (8 to 16 characters):********
 Enter the new password again for confirmation:********
Success.

DWS-3160-24PC:admin#
```

15-17 delete captive_portal user

Description

This command is used to delete a specific Captive Portal users from the local user database or to delete them all.

Format

delete captive_portal user [all | <int 1-128>]

Parameters

all - Specifies that all captive portal users will be deleted.

<int 1-128> - Enter the user ID, of a specific captive portal user to be deleted, here. This value must be between 1 and 128.

Restrictions

Only Administrators can issue this command.

Example

To delete a specific Captive Portal user:

```
DWS-3160-24PC:admin#delete captive_portal user 3
Command: delete captive_portal user 3

Success.

DWS-3160-24PC:admin#
```

15-18 config captive_portal user

Description

This command is used to configure Captive Portal users in the local database.

Format

config captive_portal user <int 1-128> [group [add <int 1-10> | delete <int 1-10>] | idle_timeout [<int 0-900> | default] | max_bandwidth_down [<int 0-536870911> | default] | max_bandwidth_up [<int 0-536870911> | default] | max_input_octets [<uint 0-4294967295> | default] | max_output_octets [<uint 0-4294967295> | default] | max_total_octets [<uint 0-4294967295> | default] | name <name 32> | password {encrypted <password 128>} | session_timeout [<int 0-86400> | default]]

Parameters

<int 1-128> - Enter the User ID used here. This value must be between 1 and 128.

group - Specifies to add or delete the group ID of the associated Captive Portal user.

add - Specifies to add a group ID to the associated Captive Portal user.

<int 1-10> - Enter the group ID value used here. This value must be between 1 and 10.

delete - Specifies to delete a group ID from the associated Captive Portal user.

<int 1-10> - Enter the group ID value used here. This value must be between 1 and 10.

idle_timeout - Specifies the idle timeout value for the associated Captive Portal user.

<int 0-900> - Enter the idle timeout value used here. This value must be between 0 and 900 seconds. The value 0 indicates that this timeout option will be disabled. The default value is 0.

default - Specifies that the default value will be used.

max_bandwidth_down - Specifies the maximum bandwidth at which the client can receive data from the network.

<int 0-536870911> - Enter the maximum down bandwidth value used here. This value must be between 0 and 536870911 bytes per second. The value 0 indicates that the default value will be used.

default - Specifies that the default value will be used.

max_bandwidth_up - Specifies the maximum bandwidth at which the client can send data into the network.

<int 0-536870911> - Enter the maximum up bandwidth value used here. This value must be between 0 and 536870911 bytes per second. The value 0 indicates that the default value will be used.

default - Specifies that the default value will be used.

max_input_octets - Specifies to limit the number of octets in bytes that the user is allowed to receive. After this limit has been reached, the user will be disconnected.

<uint 0-4294967295> - Enter the maximum input octets value used here. This value must be between 0 and 4294967295 bytes. The value 0 indicates to denote unlimited transmission. The default value is 0.

default - Specifies that the default value will be used.

max_output_octets - Specifies to limit the number of octets in bytes that the user is allowed to transmit. After this limit has been reached, the user will be disconnected.

<uint 0-4294967295> - Enter the maximum output octets value used here. This value must be between 0 and 4294967295 bytes. The value 0 indicates to denote unlimited transmission. The default value is 0.

default - Specifies that the default value will be used.

max_total_octets - Specifies to limit the number of octets in bytes that the user is allowed to transmit and receive. The maximum number of octets is the sum of the octets transmitted and received. After this limit has been reached, the user will be disconnected.

<uint 0-4294967295> - Enter the maximum total octets value used here. This value must be between 0 and 4294967295 bytes. The value 0 indicates to denote unlimited transmission. The default value is 0.

default - Specifies that the default value will be used.

name - Specifies the name of the user ID.

<name 32> - Enter the user’s ID name used here. This name can be up to 32 characters long.

password - Specifies the password of the associated Captive Portal user.

encrypted - (Optional) Specifies that the password will be in the encrypted format.

<password 128> - Enter the user password used here. This password can be up to 128 hexadecimal characters long.

session_timeout - Specifies the session timeout value for the associated Captive Portal user.

<int 0-86400> - Enter the session timeout value used here. This value must be between 0 and 86400 seconds. The value of 0, indicates that this timeout option will not be enforced. The default value is 0.

default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To assign the group 2 to the associated Captive Portal user 1:

```
DWS-3160-24PC:admin#config captive_portal user 1 group add 2
Command: config captive_portal user 1 group add 2

Success.

DWS-3160-24PC:admin#
```

To configure a name for a Captive Portal user:

```
DWS-3160-24PC:admin#config captive_portal user 1 name CPuser
Command: config captive_portal user 1 name CPuser

Success.

DWS-3160-24PC:admin#
```

To configure the password for a Captive Portal user:

```
DWS-3160-24PC:admin#config captive_portal user 1 password
Command: config captive_portal user 1 password

 Enter a case-sensitive new password (8 to 16 characters):********
 Enter the new password again for confirmation:********
Success.

DWS-3160-24PC:admin#
```

To configure the session timeout value for a Captive Portal user:

```
DWS-3160-24PC:admin#config captive_portal user 1 session_timeout 600
Command: config captive_portal user 1 session_timeout 600

Success.

DWS-3160-24PC:admin#
```

To configure the maximum bandwidth up value for a Captive Portal user:

```
DWS-3160-24PC:admin#config captive_portal user 1 max_bandwidth_up 102400
Command: config captive_portal user 1 max_bandwidth_up 102400

Success.

DWS-3160-24PC:admin#
```

15-19 show captive_portal user

Description

This command is used to display all configured users or a specific user in the Captive Portal local user database on the Switch.

Format

show captive_portal user {<int 1-128>}

Parameters

<int 1-128> - (Optional) Enter the user ID used here. This value must be between 1 and 128.

Restrictions

None.

Example

To display the information of all Captive Portal users:

```
DWS-3160-24PC:admin#show captive_portal user
Command: show captive_portal user

                              Session  Idle
User ID       User Name       Timeout Timeout  Group ID      Group Name
------- --------------------- ------- -------- -------- ---------------------
1       CPuser                600     0        1        Default
                                               2
2       newuser               0       0        1        Default

Total Users: 2

DWS-3160-24PC:admin#
```

To display the information of Captive Portal user 1:

```
DWS-3160-24PC:admin#show captive_portal user 1
Command: show captive_portal user 1

User ID                                       : 1
User Name                                     : CPuser
Password Configured                           : Yes
Session Timeout                               : 600
Idle Timeout                                  : 0
Max Bandwidth Up (bytes/sec)                  : 102400
Max Bandwidth Down (bytes/sec)                : 0
Max Input Octets (bytes)                      : 0
Max Output Octets (bytes)                     : 0
Max Total Octets (bytes)                      : 0

Group ID            Group Name
-------- --------------------------------
1        Default
2

DWS-3160-24PC:admin#
```

15-20 create captive_portal user group

Description

This command is used to create a Captive Portal user group.

Format

create captive_portal user group <int 1-10>

Parameters

<int 1-10> - Enter the Captive Portal user group ID used here. This value must be between 1 and 10.

Restrictions

Only Administrators can issue this command.

Example

To create a Captive Portal user group:

```
DWS-3160-24PC:admin#create captive_portal user group 3
Command: create captive_portal user group 3

Success.

DWS-3160-24PC:admin#
```

15-21 delete captive_portal user group

Description

This command is used to delete a Captive Portal user group. The default user group ID is 1 and is not allowed to be deleted.

Format

delete captive_portal user group <int 1-10>

Parameters

<int 1-10> - Enter the Captive Portal user group ID used here. This value must be between 1 and 10.

Restrictions

Only Administrators can issue this command.

Example

To delete a Captive Portal user group:

```
DWS-3160-24PC:admin#delete captive_portal user group 3
Command: delete captive_portal user group 3

Success.

DWS-3160-24PC:admin#
```

15-22 config captive_portal user group

Description

This command is used to configure a Captive Portal user group on the Switch.

Format

config captive_portal user group <int 1-10> [name <name 32> | moveusers <int 1-10>]

Parameters

<int 1-10> - Enter the Captive Portal user group ID used here. This value must be between 1 and 10.

name - Specifies the group name.
<name 32> - Enter the group name used here. This name can be up to 32 characters long.

moveusers - Specifies to move existing users from one user group to another. Note that the destination group must already exist before a move can be successful.
<int 1-10> - Enter the Captive Portal user group ID used here. This value must be between 1 and 10.

Restrictions

Only Administrators can issue this command.

Example

To configure the name of a Captive Portal user group:

```
DWS-3160-24PC:admin#config captive_portal user group 2 name group2
Command: config captive_portal user group 2 name group2

Success.

DWS-3160-24PC:admin#
```

To move the Captive Portal users from group 1 to group 2.

```
DWS-3160-24PC:admin#config captive_portal user group 1 moveusers 2
Command: config captive_portal user group 1 moveusers 2

Success.

DWS-3160-24PC:admin#
```

15-23 show captive_portal user group

Description

This command is used to display all configured user groups or a specific user group in the Captive Portal local database.

Format

show captive_portal user group {<int 1-10>}

Parameters

<int 1-10> - (Optional) Enter the Captive Portal user group ID used here. This value must be between 1 and 10.

If no parameter is specified, then all the user groups will be displayed.

Restrictions

None.

Example

To display all the user groups in the Captive Portal local user group database:

```
DWS-3160-24PC:admin#show captive_portal user group
Command: show captive_portal user group

Group ID      Group Name       User ID       User Name
-------- --------------------- ------- ----------------------
1        Default
2        group2                1       CPuser
                               2       newuser

Total Groups: 2

DWS-3160-24PC:admin#
```

To display a specific user group in the Captive Portal local user group database:

```
DWS-3160-24PC:admin#show captive_portal user group 2
Command: show captive_portal user group 2

Group ID                                      : 2
Group Name                                    : group2

User ID            User Name
------- --------------------------------
1       CPuser

DWS-3160-24PC:admin#
```

Chapter 16 Command Logging Command List

enable command logging
disable command logging
show command logging

16-1 enable command logging

Description

This command is used to enable the command logging function. When the Switch is under the booting procedure, all configuration commands will not be logged. When the user accesses the Switch under the AAA authentication mode, the username should not changed if user uses “enable admin” command to replace its privilege.

Format

enable command logging

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the command logging function:

```
DWS-3160-24PC:admin# enable command logging
Command: enable command logging

Success.

DWS-3160-24PC:admin#
```

16-2 disable command logging

Description

This command is used to disable the command logging function.

Format

disable command logging

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the command logging:

```
DWS-3160-24PC:admin# disable command logging
Command: disable command logging

Success.

DWS-3160-24PC:admin#
```

16-3 show command logging

Description

This command is used to display the Switch’s general command logging configuration status.

Format

show command logging

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display the command logging configuration status:

```
DWS-3160-24PC:admin#show command logging
Command: show command logging

 Command Logging State: Enabled

DWS-3160-24PC:admin#
```

Chapter 17 Compound Authentication Command List

create authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
delete authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
config authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [add | delete] ports [<portlist> | all]
config authentication ports [<portlist> | all] {auth_mode [port_based | host_based {vlanid <vid_list> state [enable | disable]}] | multi_authen_methods [none | any | dot1x_impb | impb_cp | mac_impb] | cp_configuration <int 1-10>}
show authentication guest_vlan
show authentication ports {<portlist>}
enable authorization attributes
disable authorization attributes
show authorization
config authentication server failover [local | permit | block]
show authentication

17-1 create authentication guest_vlan

Description

This command is used to assign a static VLAN to be a guest VLAN. The specific VLAN which assigned to guest VLAN must be existed. The specific VLAN which assigned to guest VLAN can’t be deleted.

Format

create authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

vlan - Specifies the guest VLAN by VLAN name. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specifies the guest VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This ID must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To assign a static VLAN to be guest VLAN:

```
DWS-3160-24PC:admin# create authentication guest_vlan vlan guestVLAN
Command: create authentication guest_vlan vlan guestVLAN

Success.

DWS-3160-24PC:admin#
```

17-2 delete authentication guest_vlan

Description

This command is used to delete the guest VLAN setting, but won’t delete the static VLAN. All ports that were enabled on the guest VLAN will move to the original VLAN after deleting the guest VLAN.

Format

delete authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

vlan - Specifies the guest VLAN by VLAN name. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specifies the guest VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This ID must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete guest VLAN configuration:

```
DWS-3160-24PC:admin# delete authentication guest_vlan vlan guestVLAN
Command: delete authentication guest_vlan vlan guestVLAN

Success.

DWS-3160-24PC:admin#
```

17-3 config authentication guest_vlan

Description

This command is used to configure security port(s) as specified guest VLAN member(s).

Format

config authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [add | delete] ports [<portlist> | all]

Parameters

vlan - Assigned a VLAN as guest VLAN. The VLAN must be an existed static VLAN. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Assigned a VLAN as guest VLAN. The VLAN must be an existed static VLAN. **<vlanid 1-4094> -** Enter the VLAN ID here. This ID must be between 1 and 4094.
add - Specifies to add port list to the guest VLAN. **delete** - Specifies to delete port list from the guest VLAN.
ports - Specifies the configured port(s). **<portlist>** - Enter the list of ports to be configured here. **all** - Specifies all ports on the Switch.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure security port(s) as specified guest VLAN member:

```
DWS-3160-24PC:admin#config authentication guest_vlan vlan v3 add ports 10
Command: config authentication guest_vlan vlan v3 add ports 10

Success.

DWS-3160-24PC:admin#
```

17-4 config authentication ports

Description

This command is used to configure security port(s).

Format

config authentication ports [<portlist> | all] {auth_mode [port_based | host_based {vlanid <vid_list> state [enable | disable]}] | multi_authen_methods [none | any | dot1x_impb | impb_cp | mac_impb] | cp_configuration <int 1-10>}

Parameters

ports - Specifies port(s) to configure. **<portlist>** - Enter the list of ports to be configured here. **all** - Specifies all ports on the Switch.
auth_mode - (Optional) Specifies the authentication mode used. **port_based** - If one of the attached hosts passes the authentication, all hosts on the same port will be granted to access network. If the user fails to authorize, this port will keep trying the next authentication **host_based** – Specifies that every user can be authenticated individually. **vlanid** - (Optional) Specific authentication VLAN(s). This is useful when different VLANs on the Switch have different authentication requirements. **<vidlist>** - Enter the VLAN ID list here. **state** - (Optional) Specifies the VID list's authentication state. **enable** - Assign the specified VID list as authentication VLAN(s). **disable** - Remove the specified VID list from authentication VLAN(s). If "vlanid" is not

specified, or all VLANs is disabled, means do not care which VLAN the client comes from, the client will be authenticated if the client's MAC(not care the VLAN) is not authenticated. After the client is authenticated, the client will not be re-authenticated when received from other VLANs. All VLANs are disabled by default.

Note: When port's authorization mode is changed to port-based, previously authentication VLAN(s) on this port will be clear.

Note: Per VLAN authentication is only supported by the Captive Portal. If the compound authentication method is not set as 'none', the port will work when the authentication VLAN is disabled.

multi_authen_methods - (Optional) Specifies the method for compound authentication.

- **none** - Compound authentication is not enabled.
- **any** - If any one of the authentication method (802.1X, MAC-based Access Control, and CP) passes, then pass.
- **dot1x_impb** - Dot1x will be verified first, and then IMPB will be verified. Both authentication need to be passed.
- **impb_cp** - IMPB will be verified first, and then CP will be verified. Both authentication need to be passed.
- **mac_impb** - MAC-AC will be verified first, and then IMPB will be verified. Both authentication need to be passed.

cp_configuration – Specifies the Captive Portal configuration used.

- **<int 1-10>** - Enter the Captive Portal configuration ID used here. This value must be between 1 and 10.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the compound authentication method of all ports to any:

```
DWS-3160-24PC:admin# config authentication ports all multi_authen_methods any
Command: config authentication ports all multi_authen_methods any

Success.

DWS-3160-24PC:admin#
```

17-5 show authentication guest_vlan

Description

This command is used to display guest VLAN setting.

Format

show authentication guest_vlan

Parameters

None.

Restrictions

None.

Example

This example displays the guest VLAN setting:

```
DWS-3160-24PC:admin#show authentication guest_vlan
Command: show authentication guest_vlan

Guest VLAN VID         : 3
Guest VLAN Member Ports: 10

Guest VLAN VID         : 100
Guest VLAN Member Ports:

 Total Entries: 2

DWS-3160-24PC:admin#
```

17-6 show authentication ports

Description

This command is used to display authentication setting on port(s).

Format

show authentication ports {<portlist>}

Parameters

ports – (Optional) Display compound authentication on the specified port(s). **<portlist>** - Enter the list of ports to be configured here.
If not Specifies the port list, displays compound authentication setting of all ports.

Restrictions

None.

Example

To display the authentication setting for all the ports:

```
DWS-3160-24PC:admin#show authentication ports
Command: show authentication ports

 Port  Methods        Auth Mode  Authentication VLAN(s)  CP Configuration
 ---- -------------- ----------- --------------------- ------------------
 1    Any            Host-based                                1
 2    Any            Host-based                                1
 3    Any            Host-based                                1
 4    Any            Host-based                                1
 5    Any            Host-based                                1
 6    Any            Host-based                                1
 7    Any            Host-based                                1
 8    Any            Host-based                                1
 9    Any            Host-based                                1
 10   Any            Host-based                                1
 11   Any            Host-based                                1
 12   Any            Host-based                                1
 13   Any            Host-based                                1
 14   Any            Host-based                                1
 15   Any            Host-based                                1
 16   Any            Host-based                                1
 17   Any            Host-based                                1
 18   Any            Host-based                                1
 19   Any            Host-based                                1
 20   Any            Host-based                                1
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

17-7 enable authorization

Description

This command is used to enable authorization.

Format

enable authorization attributes

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the authorization global state:

```
DWS-3160-24PC:admin# enable authorization attributes
Command: enable authorization attributes

Success.

DWS-3160-24PC:admin#
```

17-8 disable authorization

Description

This command is used to disable authorization.

Format

disable authorization attributes

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the authorization global state:

```
DWS-3160-24PC:admin# disable authorization attributes
Command: disable authorization attributes

Success.

DWS-3160-24PC:admin#
```

17-9 show authorization

Description

This command is used to display authorization status.

Format

show authorization

Parameters

None.

Restrictions

None.

Example

To display the authorization status:

```
DWS-3160-24PC:admin#show authorization
Command: show authorization

Authorization for Attributes: Enabled

DWS-3160-24PC:admin#
```

17-10 config authentication server failover

Description

This command is used to configure authentication server failover function.

Format

config authentication server failover [local | permit | block]

Parameters

local - Use local DB to authenticate the client.
permit - The client is always regarded as authenticated.
block - Block the client (Default setting).

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the authentication server's failover state:

```
DWS-3160-24PC:admin# config authentication server failover local
Command: config authentication server failover local

Success.

DWS-3160-24PC:admin#
```

17-11 show authentication

Description

This command is used to display the global authentication configuration.

Format

show authentication

Parameters

None.

Restrictions

None.

Example

To display the global authentication configuration:

```
DWS-3160-24PC:admin# show authentication
Command: show authentication

Authentication Server Failover: Block.

DWS-3160-24PC:admin# show authentication
Command: show authentication

Authentication Server Failover: Permit.

DWS-3160-24PC:admin# show authentication
Command: show authentication

Authentication Server Failover: Local.

DWS-3160-24PC:admin#
```

Chapter 18 Configuration Command List

show config [effective | modified | current_config | boot_up | file <pathname 64>] {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}
config configuration <pathname 64> [boot_up | active]
save {[config <pathname 64> | log | all]}
show boot_file

18-1 show config

Description

This command is used to display the content of the current configuration, the configuration to be used in next boot, or the configuration file specified by the command.

The output stream of the configuration data can be filtered by the expression specified at the end of the command. The expression can contain up to three multiple filter evaluations. A filter evaluation begins with a filter type (include, exclude, and begin), followed by up to three filter strings (ex: “stp”). A filter string is enclosed by symbol ".

The following describes the meaning of the each filter type.

- include: includes lines that contain the specified filter string.
- exclude: excludes lines that contain the specified filter string
- begin: The first line that contains the specified filter string will be the first line of the output.

The relationship of multiple filter strings following the same filter type is OR. That is, one line is qualified if one of specified filter strings is matched.

If more than one filter evaluation is specified; the output of filtered by the former evaluation will be used as the input of the latter evaluation.

Format

show config [effective | modified | current_config | boot_up | file <pathname 64>] {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}

Parameters

effective - Display only commands which affects the behavior of the device. For example, if STP is disabled, then for STP configuration, only “STP is disabled” is displayed. All other lower

level setting regarding STP is not displayed. The lower level setting will only be displayed when the higher level setting is enabled.

modified - Display only the commands which are not from the 'reset' default setting.

current_config - Specifies the current configuration.

boot_up - Specifies the list of the boot-up configuration.

file - Specifies that the unit can display the specified configuration file.

<pathname 64> - The pathname specifies an absolute pathname on the device file system. If pathname is not specified, the boot up configuration is implied. This name can be up to 64 characters long.

<filter_string 80> - (Optional) A filter string is enclosed by symbol ". Thus, the filter string itself cannot contain the "character. The filter string is case sensitive. This value can be up to 80 characters long.

include - Includes lines that contain the specified filter string.

exclude - Excludes lines that contain the specified filter string

begin - The first line that contains the specified filter string will be the first line of the output.

Restrictions

Only Administrators can issue this command.

Example

The following example illustrates how the special filters 'modified' affect the configuration display:

```
DWS-3160-24PC:admin#show config modified
Command: show config modified

#-------------------------------------------------------------------------------
#                    DWS-3160-24PC Gigabit Ethernet Switch
#                                Configuration
#
#                           Firmware: Build 1.00.034
#           Copyright(C) 2012 D-Link Corporation. All rights reserved.
#-------------------------------------------------------------------------------

# DEVICE

# BASIC

# ACCOUNT LIST
create account admin admin
*@&2jmj7l5rSw0yVb/vlWAYkK/YBwmwMs6D
*@&2jmj7l5rSw0yVb/vlWAYkK/YBwmwMs6D

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

The following example illustrates how the special filters 'effective' affect the configuration display:

```
DWS-3160-24PC:admin#show config effective
Command: show config effective

#-------------------------------------------------------------------------------
#                    DWS-3160-24PC Gigabit Ethernet Switch
#                                Configuration
#
#                           Firmware: Build 1.00.034
#           Copyright(C) 2012 D-Link Corporation. All rights reserved.
#-------------------------------------------------------------------------------

# DEVICE

config temperature threshold high 79
config temperature threshold low 11
config temperature trap state enable
config temperature log state enable

# BASIC

# ACCOUNT LIST

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

18-2 config configuration

Description

This command is used to select a configuration file as the next boot up configuration or to apply a specific configuration to the system. This command is required when multiple configuration files are supported.

Format

config configuration <pathname 64> [boot_up | active]

Parameters

<pathname 64> - Specifies a configuration file on the device file system.
boot_up - (Optional) Specifies it as a boot up file. **active** - (Optional) Specifies to apply the configuration.

Restrictions

Only Administrators can issue this command.

Example

To configure the Switch’s configuration file as boot up:

```
DWS-3160-24PC:admin#config configuration config.cfg boot_up
Command: config configuration config.cfg boot_up

Success.

DWS-3160-24PC:admin#
```

18-3 save

Description

This command is used to save the current configuration to a file. This command is required to be supported regardless of whether file system is supported or whether multiple configuration files are supported. If the configuration ID or configuration file name is not specified, the next boot up configuration is implied.

Format

save {[config <pathname 64> | log | all]}

Parameters

config – Specifies to save the configuration to a file.

<pathname 64> - (Optional) The pathname specifies the absolute pathname on the device file system. If pathname is not specified, it refers to the boot up configuration file. This name can be up to 64 characters long.

log – Specifies to save the log.

all – Specifies to save the configuration and the log.

Restrictions

Only Administrators and Operators can issue this command.

Example

To save the configuration:

```
DWS-3160-24PC:admin#save config c:/config.cfg
Command: save config c:/config.cfg

Saving all configurations to NV-RAM.......... Done.

DWS-3160-24PC:admin#
```

18-4 show boot_file

Description

This command is used to display the configuration file and firmware image assigned as boot up files.

Format

show boot_file

Parameters

None.

Restrictions

None.

Example

To display the boot file:

```
DWS-3160-24PC:admin#show boot_file
Command: show boot_file

  Bootup Firmware       : /c:/runtime.had
  Bootup Configuration  : /c:/config.cfg

DWS-3160-24PC:admin#
```

Chapter 19 Connectivity Fault Management Command List

create cfm md <string 22> {md_index <uint 1-4294967295>} level <int 0-7>

config cfm md [<string 22> | md_index <uint 1-4294967295>] {mip [none | auto | explicit] | sender_id [none | chassis | manage | chassis_manage]}

create cfm ma <string 22> {ma_index <uint 1-4294967295>} md [<string 22> | md_index <uint 1-4294967295>]

config cfm ma [<string 22> | ma_index <uint 1-4294967295>] md [<string 22> | md_index <uint 1-4294967295>] {vlanid <vlanid 1-4094> | mip [none | auto | explicit | defer] | sender_id [none | chassis | manage | chassis_manage | defer] | ccm_interval [10ms | 100ms | 1sec | 10sec | 1min | 10min] | mepid_list [add | delete] <mepid_list>}

create cfm mep <string 32> mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] direction [inward | outward] port <port>

config cfm mep [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {state [enable | disable] | ccm [enable | disable] | pdu_priority <int 0-7> | fault_alarm [all | mac_status | remote_ccm | error_ccm | xcon_ccm | none] | alarm_time <centisecond 250 -1000> | alarm_reset_time <centisecond 250-1000>}

delete cfm mep [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]]

delete cfm ma [<string 22> | ma_index <uint 1-4294967295>] md [<string 22> | md_index <uint 1-4294967295>]

delete cfm md [<string 22> | md_index <uint 1-4294967295>]

enable cfm

disable cfm

config cfm ports <portlist> state [enable | disable]

show cfm ports <portlist>

show cfm {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}

show cfm fault {md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>]}}

show cfm port <port> {level <int 0-7> | direction [inward | outward] | vlanid <vlanid 1-4094>}

cfm loopback <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {num <int 1-65535> | [length <int 0-1500> | pattern <string 1500>] | pdu_priority <int 0-7>}

cfm linktrace <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {ttl <int 2-255> | pdu_priority <int 0-7>}

show cfm linktrace [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {trans_id <uint>}

delete cfm linktrace {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}

show cfm mipccm

config cfm mp_ltr_all [enable | disable]

show cfm mp_ltr_all

show cfm remote_mep [mepname <string 32> | md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191>] remote_mepid <int 1-8191>

show cfm pkt_cnt {[ports <portlist> {[rx | tx]} | [rx | tx] | ccm]}

clear cfm pkt_cnt {[ports <portlist> {[rx | tx]} | [rx | tx] | ccm]}

19-1 create cfm md

Description

This command is used to create a maintenance domain.

Format

create cfm md <string 22> {md_index <uint 1-4294967295>} level <int 0-7>

Parameters

md - Specifies the maintenance domain name.
<string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.

md_index - (Optional) Specifies the maintenance domain index.
<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 7294967295.

level - Specifies the maintenance domain level.
<int 0-7> - Enter the maintenance domain level here. This value must be between 0 and 7.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a maintenance domain called “op_domain” and assign a maintenance domain level of “2”:

```
DWS-3160-24PC:admin# create cfm md op_domain level 2
Command: create cfm md op_domain level 2

Success.

DWS-3160-24PC:admin#
```

19-2 config cfm md

Description

This command is used to configure the parameters of a maintenance domain. The creation of MIPs on an MA is useful to trace the link, MIP by MIP. It also allows the user to perform a loopback from an MEP to an MIP.

Format

config cfm md [<string 22> | md_index <uint 1-4294967295>] {mip [none | auto | explicit] | sender_id [none | chassis | manage | chassis_manage]}

Parameters

md - Specifies the maintenance domain name.

<string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.

md_index - Specifies the maintenance domain index.
<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

mip - (Optional) This is the control creations of MIPs.
none - Do not create MIPs. This is the default value.
auto - MIPs can always be created on any ports in this MD, if that port is not configured with an MEP of this MD. For the intermediate Switch in an MA, the setting must be automatic in order for the MIPs to be created on this device.
explicit - MIPs can be created on any ports in this MD, only if the next existent lower level has an MEP configured on that port, and that port is not configured with an MEP of this MD.

sender_id - (Optional) This is the control transmission of the sender ID TLV.
none - Do not transmit the sender ID TLV. This is the default value.
chassis - Transmit the sender ID TLV with the chassis ID information.
manage - Transmit the sender ID TLV with the managed address information.
chassis_manage - Transmit sender ID TLV with chassis ID information and manage address information.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the maintenance domain called “op_domain” and Specifies the explicit option for creating MIPs:

```
DWS-3160-24PC:admin# config cfm md op_domain mip explicit
Command: config cfm md op_domain mip explicit

Success.

DWS-3160-24PC:admin#
```

19-3 create cfm ma

Description

This command is used to create a maintenance association. Different MAs in an MD must have different MA Names. Different MAs in different MDs may have the same MA Name.

Format

create cfm ma <string 22> {ma_index <uint 1-4294967295>} md [<string 22> | md_index <uint 1-4294967295>]

Parameters

ma - Specifies the maintenance association name.
<string 22> - Enter the maintenance association name here. This name can be up to 22 characters long.

ma_index - (Optional) Specifies the maintenance association index.
<uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

md - Specifies the maintenance domain name.
  <string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.

md_index - Specifies the maintenance domain index.
  <uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a maintenance association called “ma” and assign it to the maintenance domain “op_domain”:

```
DWS-3160-24PC:admin# create cfm ma op1 md op_domain
Command: create cfm ma op1 md op_domain

Success.

DWS-3160-24PC:admin#
```

19-4 config cfm ma

Description

This command is used to configure the parameters of a maintenance association. The MEP list specified for an MA can be located in different devices. MEPs must be created on the ports of these devices explicitly. An MEP will transmit a CCM packet periodically across the MA. The receiving MEP will verify these received CCM packets from the other MEPs against this MEP list for the configuration integrity check.

Format

config cfm ma [<string 22> | ma_index <uint 1-4294967295>] md [<string 22> | md_index <uint 1-4294967295>] {vlanid <vlanid 1-4094> | mip [none | auto | explicit | defer] | sender_id [none | chassis | manage | chassis_manage | defer] | ccm_interval [10ms | 100ms | 1sec | 10sec | 1min | 10min] | mepid_list [add | delete] <mepid_list>}

Parameters

ma - Specifies the maintenance association name.
  <string 22> - Enter the maintenance association name here. This name can be up to 22 characters long.

ma_index - Specifies the maintenance association index.
  <uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

md - Specifies the maintenance domain name.
  <string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.

md_index - Specifies the maintenance domain index.
  <uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

vlanid - (Optional) Specifies the VLAN Identifier. Different MAs must be associated with different VLANs.
<vlanid 1-4094> - Enter the VLAN ID used here. This value must be between 1 and 4094.

mip - (Optional) This is the control creation of MIPs.
none - Specifies not to create MIPs.
auto - MIPs can always be created on any ports in this MA, if that port is not configured with an MEP of that MA.
explicit - MIP can be created on any ports in this MA, only if the next existing lower level has an MEP configured on that port, and that port is not configured with an MEP of this MA.
defer - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.

sender_id - (Optional) This is the control transmission of the sender ID TLV.
none - Do not transmit the sender ID TLV. This is the default value.
chassis - Transmit the sender ID TLV with the chassis ID information.
manage - Transmit the sender ID TLV with the manage address information.
chassis_manage - Transmit the sender ID TLV with the chassis ID information and the manage address information.
defer - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.

ccm_interval - (Optional) This is the CCM interval.
10ms - Specifies that the CCM interval will be set to 10 milliseconds. Not recommended.
100ms - Specifies that the CCM interval will be set to 100 milliseconds. Not recommended.
1sec - Specifies that the CCM interval will be set to 1 second.
10sec - Specifies that the CCM interval will be set to 10 seconds. This is the default value.
1min - Specifies that the CCM interval will be set to 1 minute.
10min - Specifies that the CCM interval will be set to 10 minutes.

mepid_list - (Optional) This is to Specifies the MEPIDs contained in the maintenance association. The range of the MEPID is 1-8191.
add - Specifies to add MEPID(s).
delete - Specifies to delete MEPID(s). By default, there is no MEPID in a newly created maintenance association.
<mepid_list> - Enter the MEP ID list here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a CFM MA:

```
DWS-3160-24PC:admin# config cfm ma op1 md op_domain vlanid 1 ccm_interval 1sec
Command: config cfm ma op1 md op_domain vlanid 1 ccm_interval 1sec

Success.

DWS-3160-24PC:admin#
```

19-5 create cfm mep

Description

This command is used to create an MEP. Different MEPs in the same MA must have a different MEPID. MD name, MA name, and MEPID that together identify a MEP.

Different MEPs on the same device must have a different MEP name. Before creating an MEP, its MEPID should be configured in the MA’s MEPID list.

Format

create cfm mep <string 32> mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] direction [inward | outward] port <port>

Parameters

mep - Specifies the MEP name. It is unique among all MEPs configured on the device.
<string 32> - Enter the MEP name used here. This name can be up to 32 characters long.

mepid - Specifies the MEP ID. It should be configured in the MA's MEPID list.
<int 1-8191> - Enter the MEP ID used here. This value must be between 1 and 8191.

md - Specifies the maintenance domain name.
<string 22> - Enter the maintenance domain name used here. This name can be up to 22 characters long.

md_index - Specifies the maintenance domain index.
<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

ma - Specifies the maintenance association name.
<string 22> - Enter the maintenance association name used here. This name can be up to 22 characters long.

ma_index - Specifies the maintenance association index.
<uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

direction - This is the MEP direction.
inward - Specifies the inward facing (up) MEP.
outward - Specifies the outward facing (down) MEP.

port - Specifies the port number. This port should be a member of the MA's associated VLAN.
<port> - Enter the port number used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a CFM MEP:

```
DWS-3160-24PC:admin# create cfm mep mep1 mepid 1 md op_domain ma op1 direction
inward port 2
Command: create cfm mep mep1 mepid 1 md op_domain ma op1 direction inward port
2


Success.


DWS-3160-24PC:admin#
```

19-6 config cfm mep

Description

This command is used to configure the parameters of an MEP.

An MEP may generate 5 types of Fault Alarms, as displayed below by their priorities from high to low:

- Cross-connect CCM Received: priority 5
- Error CCM Received: priority 4
- Some Remote MEPs Down: priority 3
- Some Remote MEP MAC Status Errors: priority 2
- Some Remote MEP Defect Indications: priority 1

If multiple types of the fault occur on an MEP, only the fault with the highest priority will be alarmed.

Format

config cfm mep [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {state [enable | disable] | ccm [enable | disable] | pdu_priority <int 0-7> | fault_alarm [all | mac_status | remote_ccm | error_ccm | xcon_ccm | none] | alarm_time <centisecond 250 -1000> | alarm_reset_time <centisecond 250-1000>}

Parameters

mepname - Specifies the MEP name.
<string 32> - Enter the MEP name used here. This name can be up to 32 characters long.

mepid - Specifies the MEP ID.
<int 1-8191> - Enter the MEP ID used here. This value must be between 1 and 8191.

md - Specifies the maintenance domain name.
<string 22> - Enter the maintenance domain name used here. This name can be up to 22 characters long.

md_index - Specifies the maintenance domain index.
<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

ma - Specifies the maintenance association name.
<string 22> - Enter the maintenance association name used here. This name can be up to 22 characters long.

ma_index - Specifies the maintenance association index.
<uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

state - (Optional) This is the MEP administrative state.
enable - Specifies that the MEP will be enabled.
disable - Specifies that the MEP will be disabled. This is the default value.

ccm - (Optional) This is the CCM transmission state.
enable - Specifies that the CCM transmission will be enabled.
disable - Specifies that the CCM transmission will be disabled. This is the default value.

pdu_priority - (Optional) The 802.1p priority is set in the CCMs and the LTMs messages transmitted by the MEP. The default value is 7.
<int 0-7> - Enter the PDU priority value here. This value must be between 0 and 7.

fault_alarm - (Optional) This is the control types of the fault alarms sent by the MEP.
all - All types of fault alarms will be sent.
mac_status - Only the fault alarms whose priority is equal to or higher than “Some Remote MEP MAC Status Errors” are sent.
remote_ccm - Only the fault alarms whose priority is equal to or higher than “Some Remote MEPs Down” are sent.
error_ccm - Only the fault alarms whose priority is equal to or higher than “Error CCM Received” are sent.
xcon_ccm - Only the fault alarms whose priority is equal to or higher than “Cross-connect CCM Received” are sent.
none - No fault alarm is sent. This is the default value.

alarm_time - (Optional) This is the time that a defect must exceed before the fault alarm can be

sent. The unit is centisecond, the range is 250-1000. The default value is 250.
<centisecond 250-1000> - Enter the alarm time value here. This value must be between 250 and 1000 centiseconds.

alarm_reset_time - (Optional) This is the dormant duration time before a defect is triggered before the fault can be re-alarmed. The unit is centisecond, the range is 250-1000. The default value is 1000.
<centisecond 250-1000> - Enter the alarm reset time value here. This value must be between 250 and 1000 centiseconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a CFM MEP:

```
DWS-3160-24PC:admin# config cfm mep mepname mep1 state enable ccm enable
Command: config cfm mep mepname mep1 state enable ccm enable

Success.

DWS-3160-24PC:admin#
```

19-7 delete cfm mep

Description

This command is used to delete a previously created MEP.

Format

delete cfm mep [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]]

Parameters

mepname - Specifies the MEP name.
<string 32> - Enter the MEP name used here. This name can be up to 32 characters long.

mepid - Specifies the MEP ID.
<int 1-8191> - Enter the MEP ID used here. This value must be between 1 and 8191.

md - Specifies the maintenance domain name.
<string 22> - Enter the maintenance domain name used here. This name can be up to 22 characters long.

md_index - Specifies the maintenance domain index.
<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

ma - Specifies the maintenance association name.
<string 22> - Enter the maintenance association name used here. This name can be up to 22 characters long.

ma_index - Specifies the maintenance association index.
<uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a CFM MEP:

```
DWS-3160-24PC:admin# delete cfm mep mepname mep1
Command: delete cfm mep mepname mep1

Success.

DWS-3160-24PC:admin#
```

19-8 delete cfm ma

Description

This command is used to delete a created maintenance association. All MEPs created in the maintenance association will be deleted automatically.

Format

delete cfm ma [<string 22> | ma_index <uint 1-4294967295>] md [<string 22> | md_index <uint 1-4294967295>]

Parameters

ma - Specifies the maintenance association name.
  <string 22> - Enter the maintenance association name used here. This name can be up to 22 characters long.

ma_index - Specifies the maintenance association index.
  <uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

md - Specifies the maintenance domain name.
  <string 22> - Enter the maintenance domain name used here. This name can be up to 22 characters long.

md_index - Specifies the maintenance domain index.
  <uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a CFM MA:

```
DWS-3160-24PC:admin# delete cfm ma op1 md op_domain
Command: delete cfm ma op1 md op_domain

Success.

DWS-3160-24PC:admin#
```

19-9 delete cfm md

Description

This command is used to delete a previously created maintenance domain. All the MEPs and maintenance associations created in the maintenance domain will be deleted automatically.

Format

delete cfm md [<string 22> | md_index <uint 1-4294967295>]

Parameters

md - Specifies the maintenance domain name. **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long.
md_index - Specifies the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a CFM MD:

```
DWS-3160-24PC:admin# delete cfm md op_domain
Command: delete cfm md op_domain

Success.

DWS-3160-24PC:admin#
```

19-10 enable cfm

Description

This command is used to enable the CFM globally.

Format

enable cfm

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the CFM globally:

```
DWS-3160-24PC:admin# enable cfm
Command: enable cfm

Success.

DWS-3160-24PC:admin#
```

19-11 disable cfm

Description

This command is used to disable the CFM globally.

Format

disable cfm

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the CFM globally:

```
DWS-3160-24PC:admin# disable cfm
Command: disable cfm

Success.

DWS-3160-24PC:admin#
```

19-12 config cfm ports

Description

This command is used to enable or disable the CFM function on a per-port basis. By default, the CFM function is disabled on all ports.

If the CFM is disabled on a port:

1. MIPs are never created on that port.
2. MEPs can still be created on that port, and the configuration can be saved.
3. MEPs created on that port can never generate or process CFM PDUs. If the user issues a Loopback or Link trace test on those MEPs, it will prompt the user to inform them that the CFM function is disabled on that port.

Format

config cfm ports <portlist> state [enable | disable]

Parameters

ports - Specifies the logical port list.
<portlist> - Enter the list of ports used for this configuration here.

state - Specifies that the CFM function will be enabled or disabled.
enable - Specifies that the CFM function will be enabled.
disable - Specifies that the CFM function will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the CFM ports:

```
DWS-3160-24PC:admin#config cfm ports 2-5 state enable
Command: config cfm ports 2-5 state enable

Success.

DWS-3160-24PC:admin#
```

19-13 show cfm ports

Description

This command is used to display the CFM state of specified ports.

Format

show cfm ports <portlist>

Parameters

ports - Specifies the logical port list.
<portlist> - Enter the list of ports used for this configuration here.

Restrictions

None.

Example

To display the CFM ports:

```
DWS-3160-24PC:admin#show cfm ports 3-6
Command: show cfm ports 3-6

Port   State
-----  --------
3      Disabled
4      Enabled
5      Enabled
6      Disabled

DWS-3160-24PC:admin#
```

19-14 show cfm

Description

This command is used to display the CFM configuration.

Format

show cfm {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}

Parameters

md - (Optional) Specifies the maintenance domain name.
<string 22> - Enter the maintenance domain name used here. This name can be up to 22 characters long.

md_index - (Optional) Specifies the maintenance domain index.
<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

ma - (Optional) Specifies the maintenance association name.
<string 22> - Enter the maintenance association name used here. This name can be up to 22 characters long.

ma_index - (Optional) Specifies the maintenance association index.
<uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

mepid - (Optional) Specifies the MEP ID.
<int 1-8191> - Enter the MEP ID used here. This value must be between 1 and 8191.

mepname - (Optional) Specifies the MEP name.
<string 32> - Enter the MEP name used here. This name can be up to 32 characters long.

Restrictions

None.

Example

To display the CFM configuration:

```
DWS-3160-24PC:admin#show cfm
Command: show cfm

CFM State: Enabled

MD Index    MD Name                 Level
----------  ----------------------  -----
1           MD                      0

DWS-3160-24PC:admin#show cfm md MD
Command: show cfm md MD

MD Index    : 1
MD Name     : MD
MD Level    : 0
MIP Creation: None
SenderID TLV: None

MA Index    MA Name                 VID
----------  ----------------------  ----
1           MA                      1

DWS-3160-24PC:admin#show cfm md MD ma MA
Command: show cfm md MD ma MA

MA Index    : 1
MA Name     : MA
MA VID      : 1
MIP Creation: Defer
CCM Interval: 10 seconds
SenderID TLV: Defer
MEPID List  : 1

MEPID  Direction  Port   Name         MAC Address
-----  ---------  -----  -----------  -----------------
1      Inward     1      MEP          00-11-22-33-45-77

DWS-3160-24PC:admin#show cfm mepname MEP
Command: show cfm mepname MEP

Name                : MEP
MEPID               : 1
Port                : 1
Direction           : Inward
CFM Port Status     : Disabled
```

```
MAC Address         : 00-11-22-33-45-77
MEP State           : Disabled
CCM State           : Disabled
PDU Priority        : 7
Fault Alarm         : Disabled
Alarm Time          : 250 centisecond((1/100)s)
Alarm Reset Time    : 1000 centisecond((1/100)s)
Highest Fault       : None
AIS State           : Disabled
AIS Period          : 1 Second
AIS Client Level    : Invalid
AIS Status          : Not Detected
LCK State           : Disabled
LCK Period          : 1 Second
LCK Client Level    : Invalid
LCK Status          : Not Detected
Out-of-Sequence CCMs: 0 received
Cross-connect CCMs  : 0 received
Error CCMs          : 0 received
Normal CCMs         : 0 received
Port Status CCMs    : 0 received
If Status CCMs      : 0 received
CCMs transmitted    : 0
In-order LBRs       : 0 received
Out-of-order LBRs   : 0 received
Next LTM Trans ID   : 0
Unexpected LTRs     : 0 received
LBMs Transmitted    : 0
AIS PDUs            : 0 received
AIS PDUs Transmitted: 0
LCK PDUs            : 0 received
LCK PDUs Transmitted: 0

DWS-3160-24PC:admin#
```

19-15 show cfm fault

Description

This command is used to display all the fault conditions detected by the MEPs contained in the specified MA or MD. This display provides the overview of the fault status by MEPs.

Format

show cfm fault {md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>]}}

Parameters

md - (Optional) Specifies the maintenance domain name.
<string 22> - Enter the maintenance domain name used here. This name can be up to 22 characters long.

md_index - (Optional) Specifies the maintenance domain index.
<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

ma - (Optional) Specifies the maintenance association name.
<string 22> - Enter the maintenance association name used here. This name can be up to 22 characters long.

ma_index - (Optional) Specifies the maintenance association index.
<uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

Restrictions

None.

Example

To display the CFM faults:

```
DWS-3160-24PC:admin# show cfm fault
Command: show cfm fault

MD Name     MA Name     MEPID Status                 AIS Status   LCK Status
----------- ----------- ----- ---------------------- ------------ ------------
op_domain   op1         1     Cross-connect          CCM          Received

DWS-3160-24PC:admin#
```

19-16 show cfm port

Description

This command is used to display MEPs and MIPs created on a port.

Format

show cfm port <port> {level <int 0-7> | direction [inward | outward] | vlanid <vlanid 1-4094>}

Parameters

port - Specifies the port number used.
<port> - Enter the port number used here.

level - (Optional) Specifies the MD Level. If not specified, all levels are displayed.
<int 0-7> - Enter the MD level value here. This value must be between 0 and 7.

direction - (Optional) Specifies the MEP direction.
inward - Specifies that the MEP direction will be inward facing.
outward - Specifies that the MEP direction will be outward facing.
If not specified, both directions and the MIP are displayed.

vlanid - (Optional) Specifies the VLAN identifier. If not specified, all VLANs are displayed.
<vlanid 1-4094> - Enter the VLAN ID used here. This value must be between 1 and 4094.

Restrictions

None.

Example

To display the MEPs and MIPs created on a port:

```
DWS-3160-24PC:admin# show cfm port 1
Command: show cfm port 1

MAC Address: 00-05-78-82-32-01

MD Name     MA Name     MEPID Level Direction VID
----------- ----------- ----- ----- --------- ----
op_domain   op1         1     2     inward    2
cust_domain cust1       8     4     inward    2
serv_domain serv2       MIP   3               2

DWS-3160-24PC:admin#
```

19-17 cfm loopback

Description

This command is used to start a CFM loopback test. You can press Ctrl+C to exit the loopback test. The MAC address represents the destination MEP or MIP that can be reached by this MAC address. The MEP represents the source MEP to initiate the loopback message.

Format

cfm loopback <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {num <int 1-65535> | [length <int 0-1500> | pattern <string 1500>] | pdu_priority <int 0-7>}

Parameters

<macaddr> - Enter the destination MAC address here.

mepname – (Optional) Specifies the MEP name used.
<string 32> - Enter the MEP name used here. This name can be up to 32 characters long.

mepid – (Optional) Specifies the MEP ID used.
<int 1-8191> - Enter the MEP ID used here. This value must be between 1 and 8191.

md – (Optional) Specifies the maintenance domain name.
<string 22> - Enter the maintenance domain name her. This name can be up to 22 characters long.

md_index – (Optional) Specifies the maintenance domain index.
<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

ma – (Optional) Specifies the maintenance association name.
<string 22> - Enter the maintenance association name her. This name can be up to 22 characters long.

ma_index – (Optional) Specifies the maintenance association index.
<uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

num - (Optional) Number of LBMs to be sent. The default value is 4.
<int 1-65535> - Enter the number of LBMs to be sent here. This value must be between 1 and 65535.

length - (Optional) The payload length of the LBM to be sent. The default is 0.
<int 0-1500> - Enter the payload length here. This value must be between 0 and 1500.

pattern - (Optional) An arbitrary amount of data to be included in a Data TLV, along with an indication whether the Data TLV is to be included.
<string 1500> - Enter the pattern used here. This value can be up to 1500 characters long.

pdu_priority - (Optional) The 802.1p priority to be set in the transmitted LBMs. If not specified, it uses the same priority as CCMs and LTMs sent by the MA.
<int 0-7> - Enter the PDU priority value here. This value must be between 0 and 7.

Restrictions

None.

Example

To transmit a LBM:

```
DWS-3160-24PC:admin# cfm loopback 00-01-02-03-04-05 mepname mep1
Command: cfm loopback 00-01-02-03-04-05 mepname mep1

Request timed out.
Request timed out.
Reply from MPID 52: bytes=xxx time=xxxms
Request timed out.

CFM loopback statistics for 00-01-02-03-04-05:
    Packets: Sent=4, Received=1, Lost=3(75% loss).

DWS-3160-24PC:admin#
```

19-18 cfm linktrace

Description

This command is used to issue a CFM link track message.

Format

cfm linktrace <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {ttl <int 2-255> | pdu_priority <int 0-7>}

Parameters

<macaddr> - Specifies the destination MAC address.

mepname – (Optional) Specifies the MEP name used.
<string 32> - Enter the MEP name used here. This name can be up to 32 characters long.

mepid – (Optional) Specifies the MEP ID used.
<int 1-8191> - Enter the MEP ID used here. This value must be between 1 and 8191.

md – (Optional) Specifies the maintenance domain name.
<string 22> - Enter the maintenance domain name her. This name can be up to 22 characters long.

md_index – (Optional) Specifies the maintenance domain index.
<uint 1-4294967295> - Enter the maintenance domain index value here. This value can be between 1 and 4294967295.

ma – (Optional) Specifies the maintenance association name.

<string 22> - Enter the maintenance association name her. This name can be up to 22 characters long.

ma_index – (Optional) Specifies the maintenance association index.
<uint 1-4294967295> - Enter the maintenance association index value here. This value can be between 1 and 4294967295.

ttl - (Optional) Specifies the link trace message TTL value. The default value is 64.
<int 2-255> - Enter the link trace message TTL value here. This value must be between 2 and 255.

pdu_priority - (Optional) The 802.1p priority to be set in the transmitted LTM. If not specified, it uses the same priority as CCMs sent by the MA.
<int 0-7> - Enter the PDU priority value here. This value must be between 0 and 7.

Restrictions

None.

Example

To transmit an LTM:

```
DWS-3160-24PC:admin# cfm linktrace 00-01-02-03-04-05 mepname mep1
Command: cfm linktrace 00-01-02-03-04-05 mepname mep1

Transaction ID: 26
Success.

DWS-3160-24PC:admin#
```

19-19 show cfm linktrace

Description

This command is used to display the link trace responses. The maximum link trace responses a device can hold is 128.

Format

show cfm linktrace [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {trans_id <uint>}

Parameters

mepname – (Optional) Specifies the MEP name used.
<string 32> - Enter the MEP name used here. This name can be up to 32 characters long.

mepid – (Optional) Specifies the MEP ID used.
<int 1-8191> - Enter the MEP ID used here. This value must be between 1 and 8191.

md – (Optional) Specifies the maintenance domain name.
<string 22> - Enter the maintenance domain name her. This name can be up to 22 characters long.

md_index – (Optional) Specifies the maintenance domain index.
<uint 1-4294967295> - Enter the maintenance domain index value here. This value must between 1 and 4294967295.

ma – (Optional) Specifies the maintenance association name.
<string 22> - Enter the maintenance association name her. This name can be up to 22 characters long.

ma_index – (Optional) Specifies the maintenance association index.
<uint 1-4294967295> - Enter the maintenance association index value here. This value must between 1 and 4294967295.

trans_id - (Optional) Specifies the identifier of the transaction displayed.
<uint> - Enter the transaction ID used here.

Restrictions

None.

Example

To display the link trace reply when the "all MPs reply LTRs" function is enabled:

```
DWS-3160-24PC:admin# show cfm linktrace mepname mep1 trans_id 26
Command: show cfm linktrace mepname mep1 trans_id 26

Transaction ID: 26
From MEP mep1 to 00-11-22-33-44-55
Start Time 2008-01-01 12:00:00


Hop  MEPID  MAC Address        Forwarded  Relay Action
---  -----  -----------------  ---------  ------------
1           00-22-33-44-55-66  Yes        FDB
2           00-33-44-55-66-77  Yes        MPDB
3           00-11-22-33-44-55  No         Hit

DWS-3160-24PC:admin#
```

To display the link trace reply when the "all MPs reply LTRs" function is disabled:

```
DWS-3160-24PC:admin# show cfm linktrace mep mep1 trans_id 26
Command: show cfm linktrace mep mep1 trans_id 26

Transaction ID: 26
From MEP mep1 to 00-11-22-33-44-55
Start Time 2008-01-01 12:00:00


Hop  MEPID  Ingress MAC Address  Egress MAC Address   Forwarded  Relay Action
---  -----  -------------------  -------------------  ---------  ------------
1    -      00-22-33-44-55-66    00-22-33-44-55-67    Yes        FDB
2    -      00-33-44-55-66-77    00-33-44-55-66-78    Yes        MPDB
3    X      00-44-55-66-77-88    00-11-22-33-44-55    No         Hit

DWS-3160-24PC:admin#
```

19-20 delete cfm linktrace

Description

This command is used to delete the stored link trace response data that have been initiated by the specified MEP.

Format

delete cfm linktrace {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}

Parameters

md - (Optional) Specifies the maintenance domain name.
<string 22> - Enter the maintenance domain name her. This name can be up to 22 characters long.

md_index - (Optional) Specifies the maintenance domain index.
<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

ma - (Optional) Specifies the maintenance association name.
<string 22> - Enter the maintenance association name her. This name can be up to 22 characters long.

ma_index - (Optional) Specifies the maintenance association index.
<uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

mepid - (Optional) Specifies the MEP ID used.
<int 1-8191> - Enter the MEP ID used here. This value must be between 1 and 8191.

mepname - (Optional) Specifies the MEP name used.
<string 32> - Enter the MEP name used here. This name can be up to 32 characters long.

Restrictions

None.

Example

To delete the CFM link trace reply:

```
DWS-3160-24PC:admin# delete cfm linktrace mepname mep1
Command: delete cfm linktrace mepname mep1

Success.

DWS-3160-24PC:admin#
```

19-21 show cfm mipccm

Description

This command is used to display the MIP CCM database entries. All entries in the MIP CCM database will be displayed. A MIP CCM entry is similar to a FDB which keeps the forwarding port information of a MAC entry.

Format

show cfm mipccm

Parameters

None.

Restrictions

None.

Example

To display MIP CCM database entries:

```
DWS-3160-24PC:admin# show cfm mipccm
Command: show cfm mipccm

MA          VID   MAC Address        Port
----------  ----  -----------------  -----
opma        1     01-02-03-04-05-06  2
opma        1     00-11-22-33-44-55  3

Total: 2

DWS-3160-24PC:admin#
```

19-22 config cfm mp_ltr_all

Description

This command is used to enable or disable the "all MPs reply LTRs" function.

Format

config cfm mp_ltr_all [enable | disable]

Parameters

mp_ltr_all - Specifies that the MP's reply to the LTR function will be set to all.
enable - Specifies that this function will be enabled.
disable - Specifies that this function will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the "all MPs reply LTRs" function:

```
DWS-3160-24PC:admin# config cfm mp_ltr_all enable
Command: config cfm mp_ltr_all enable

Success.

DWS-3160-24PC:admin#
```

19-23 show cfm mp_ltr_all

Description

This command is used to display the current configuration of the "all MPs reply LTRs" function.

Format

show cfm mp_ltr_all

Parameters

None.

Restrictions

None.

Example

To display the configuration of the "all MPs reply LTRs" function:

```
DWS-3160-24PC:admin# show cfm mp_ltr_all
Command: show cfm mp_ltr_all

All MPs reply LTRs: Disabled

DWS-3160-24PC:admin#
```

19-24 show cfm remote_mep

Description

This command is used to display remote MEPs.

Format

show cfm remote_mep [mepname <string 32> | md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191>] remote_mepid <int 1-8191>

Parameters

mepname – (Optional) Specifies the MEP name used.

<string 32> - Enter the MEP name used here. This name can be up to 32 characters long.

md – (Optional) Specifies the maintenance domain name.
<string 22> - Enter the maintenance domain name her. This name can be up to 22 characters long.

md_index – (Optional) Specifies the maintenance domain index.
<uint 1-4294967295> - Enter the maintenance domain index value here. This value must between 1 and 4294967295.

ma – (Optional) Specifies the maintenance association name.
<string 22> - Enter the maintenance association name her. This name can be up to 22 characters long.

ma_index – (Optional) Specifies the maintenance association index.
<uint 1-4294967295> - Enter the maintenance association index value here. This value must between 1 and 4294967295.

mepid – (Optional) Specifies the MEP ID used.
<int 1-8191> - Enter the MEP ID used here. This value must be between 1 and 8191.

remote_mepid - Specifies the Remote MEP ID used.
<int 1-8191> - Enter the remote MEP ID used here. This value must be between 1 and 8191.

Restrictions

None.

Example

To display the CFM Remote MEP information:

```
DWS-3160-24PC:admin# show cfm remote_mep mepname mep1 remote_mepid 2
Command: show cfm remote_mep mepname mep1 remote_mepid 2

Remote MEPID             : 2
MAC Address              : 00-11-22-33-44-02
Status                   : OK
RDI                      : Yes
Port State               : Blocked
Interface Status         : Down
Last CCM Serial Number   : 1000
Sender Chassis ID        : 00-11-22-33-44-00
Sender Management Address: SNMP-UDP-IPv4 10.90.90.90:161
Detect Time              : 2008-01-01 12:00:00

DWS-3160-24PC:admin#
```

19-25 show cfm pkt_cnt

Description

This command is used to display the CFM packet's RX/TX counters.

Format

show cfm pkt_cnt {[ports <portlist> {[rx | tx]} | [rx | tx] | ccm]}

Parameters

ports - (Optional) Specifies the port counters to display. If not specified, all ports will be displayed.
<portlist> - Enter the list of ports used for this configuration here.

rx - (Optional) Specifies to display the RX counter.
tx - (Optional) Specifies to display the TX counter. If not specified, both of them will be displayed.

rx - (Optional) Specifies to display the RX counter.
tx - (Optional) Specifies to display the TX counter. If not specified, both of them will be displayed.

ccm - (Optional) Specifies the CCM RX counters.

Restrictions

None.

Example

To display the CFM packet’s RX/TX counters:

```
DWS-3160-24PC:admin# show cfm pkt_cnt
Command: show cfm pkt_cnt

CFM RX Statistics
-----------------------------------------------------------------------------
Port  AllPkt   CCM      LBR      LBM     LTR      LTM      VidDrop OpcoDrop
----- -------- -------- -------- -------- -------- -------- -------- --------
all   204      204      0        0        0        0        0        0
1     0        0        0        0        0        0        0        0
2     204      204      0        0        0        0        0        0
3     0        0        0        0        0        0        0        0
4     0        0        0        0        0        0        0        0
5     0        0        0        0        0        0        0        0
6     0        0        0        0        0        0        0        0
7     0        0        0        0        0        0        0        0
8     0        0        0        0        0        0        0        0
9     0        0        0        0        0        0        0        0
10    0        0        0        0        0        0        0        0
11    0        0        0        0        0        0        0        0
12    0        0        0        0        0        0        0        0

CFM TX Statistics
-----------------------------------------------------------
Port  AllPkt   CCM      LBR      LBM      LTR      LTM
----- -------- -------- -------- -------- -------- --------
all   3988     3984     0        0        0        4
1     0        0        0        0        0        0
2     204      204      0        0        0        4
3     578      578      0        0        0        0
4     578      578      0        0        0        0
5     578      578      0        0        0        0
6     578      578      0        0        0        0
7     578      578      0        0        0        0
8     578      578      0        0        0        0
9     578      578      0        0        0        0
```

```
10    578      578      0        0        0        0
11    578      578      0        0        0        0
12    578      578      0        0        0        0

DWS-3160-24PC:admin# show cfm pkt_cnt ccm
Command: show cfm pkt_cnt ccm

CCM RX counters:
XCON   = Cross-connect CCMs
Error  = Error CCMs
Normal = Normal CCMs

MEP Name     VID  Port   Level  Direction XCON         Error       Normal
----------- ---- ----- -----  --------- ---------- ---------- ----------
mep1          1    1     2        inward    9            8           100
mep2          1    2     2        inward    9            8           100
mep3          1    3     2        inward    9            8           100
                             -----------------------------------------
                                    Total:    27            24          300

DWS-3160-24PC:admin#
```

19-26 clear cfm pkt_cnt

Description

This command is used to clear the CFM packet’s RX/TX counters.

Format

clear cfm pkt_cnt {[ports <portlist> {[rx | tx]} | [rx | tx] | ccm]}

Parameters

ports - (Optional) The ports which require need the counters clearing. If not specified, all ports will be cleared.
<portlist> - Enter the list of ports used for this configuration here.

rx - (Optional) Specifies to clear the RX counter.
tx - (Optional) Specifies to clear the TX counter. If not specified, both of them will be cleared.

rx - (Optional) Specifies to clear the RX counter.
tx - (Optional) Specifies to clear the TX counter. If not specified, both of them will be cleared.

ccm - (Optional) Specifies the CCM RX counters.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear the CFM packet’s RX/TX counters:

```
DWS-3160-24PC:admin#clear cfm pkt_cnt
Command: clear cfm pkt_cnt

Success.

DWS-3160-24PC:admin#clear cfm pkt_cnt ccm
Command: clear cfm pkt_cnt ccm

Success.

DWS-3160-24PC:admin#
```

Chapter 20 Connectivity Fault Management (CFM) Extension Command List

config cfm ais md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> {period [1sec | 1min] | level <int 0-7> | state [enable | disable]}

config cfm lock md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> {period [1sec | 1min] | level <int 0-7> | state [enable | disable]}

cfm lock md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> remote_mepid <int 1-8191> action [start | stop]

config cfm ccm_fwd [software | hardware]

show cfm ccm_fwd

20-1 config cfm ais

Description

This command is used to configure the parameters of AIS function on a MEP. The default client MD level is MD level at which the most immediate client layer MIPs and MEPs exist.

NOTE: This default client MD level is not a fixed value. It may change when creating or deleting higher level MDs and MAs on the device.

When the most immediate client layer MIPs and MEPs do not exist, the default client MD level cannot be calculated. If the default client MD level cannot be calculated and user doesn’t designate a client level, the AIS and LCK PDU cannot be transmitted.

Format

config cfm ais md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> {period [1sec | 1min] | level <int 0-7> | state [enable | disable]}

Parameters

md - Specifies the maintenance domain name.
<string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.

md_index – (Optional) Specifies the maintenance domain index.
<uint 1-4294967295> - Enter the maintenance domain index value here. This value must between 1 and 4294967295.

ma - Specifies the maintenance association name.
<string 22> - Enter the maintenance association name here. This name can be up to 22 characters long.

ma_index – (Optional) Specifies the maintenance association index.
<uint 1-4294967295> - Enter the maintenance association index value here. This value must between 1 and 4294967295.

mepid - The MEP ID in the MD which sends AIS frame.
    <int 1-8191> - Enter the MEP ID value here. This value must be between 1 and 8191.

period - (Optional) The transmitting interval of AIS PDU. The default period is 1 second.
    1sec - Specifies that the transmitting interval will be set to 1 second.
    1min - Specifies that the transmitting interval will be set to 1 minute.

level - (Optional) The client level ID to which the MEP sends AIS PDU. The default client MD level is MD level at which the most immediate client layer MIPs and MEPs exist.
    <int 0-7> - Enter the client level ID here. This value must be between 0 and 7.

state - (Optional) Specifies to enable or disable the AIS function.
    enable - Specifies that the AIS function will be enabled.
    disable - Specifies that the AIS function will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the AIS function enabled and client level is 5:

```
DWS-3160-24PC:admin# config cfm ais md op-domain ma op-ma mepid 1 state enable
level 5
Command: config cfm ais md op-domain ma op-ma mepid 1 state enable level 5

Success.

DWS-3160-24PC:admin#
```

20-2 config cfm lock

Description

This command is used to configure the parameters of LCK function on a MEP. The default client MD level is MD level at which the most immediate client layer MIPs and MEPs exist.

NOTE: This default client MD level is not a fixed value. It may change when creating or deleting higher level MD and MA on the device.

When the most immediate client layer MIPs and MEPs do not exist, the default client MD level cannot be calculated. If the default client MD level cannot be calculated and user doesn't designate a client level, the AIS and LCK PDU cannot be transmitted.

Format

config cfm lock md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> {period [1sec | 1min] | level <int 0-7> | state [enable | disable]}

Parameters

md - Specifies the maintenance domain name.
    <string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.

md_index – (Optional) Specifies the maintenance domain index.
<uint 1-4294967295> - Enter the maintenance domain index value here. This value must between 1 and 4294967295.

ma - Specifies the maintenance association name.
<string 22> - Enter the maintenance association name here. This name can be up to 22 characters long.

ma_index – (Optional) Specifies the maintenance association index.
<uint 1-4294967295> - Enter the maintenance association index value here. This value must between 1 and 4294967295.

mepid - The MEP ID in the MD which sends LCK frame.
<int 1-8191> - Enter the MEP ID value here. This value must be between 1 and 8191.

period - (Optional) The transmitting interval of LCK PDU. The default period is 1 second.
1sec - Specifies that the transmitting interval will be set to 1 second.
1min - Specifies that the transmitting interval will be set to 1 minute.

level - (Optional) The client level ID to which the MEP sends LCK PDU. The default client MD level is MD level at which the most immediate client layer MIPs and MEPs exist.
<int 0-7> - Enter the client level ID here. This value must be between 0 and 7.

state - (Optional) Specifies to enable or disable the LCK function.
enable - Specifies that the LCK function will be enabled.
disable - Specifies that the LCK function will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the LCK function enabled and client level is 5:

```
DWS-3160-24PC:admin# config cfm lock md op-domain ma op-ma mepid 1 state enable
level 5
Command: config cfm lock md op-domain ma op-ma mepid 1 state enable level 5

Success.

DWS-3160-24PC:admin#
```

20-3 cfm lock md

Description

This command is used to start/stop cfm management lock. This command will result in the MEP sends a LCK PDU to client level MEP.

Format

cfm lock md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> remote_mepid <int 1-8191> action [start | stop]

Parameters

md - Specifies the maintenance domain name.
<string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.

md_index – (Optional) Specifies the maintenance domain index.

<uint 1-4294967295> - Enter the maintenance domain index value here. This value must between 1 and 4294967295.

ma - Specifies the maintenance association name.
<string 22> - Enter the maintenance association name here. This name can be up to 22 characters long.

ma_index – (Optional) Specifies the maintenance association index.
<uint 1-4294967295> - Enter the maintenance association index value here. This value must between 1 and 4294967295.

mepid - The MEP ID in the MD which sends LCK frame.
<int 1-8191> - Enter the MEP ID value here. This value must be between 1 and 8191.

remote_mepid - The peer MEP is the target of management action.
<int 1-8191> - Enter the remote MEP ID used here. This value must be between 1 and 8191.

action - Specifies to start or to stop the management lock function.
start - Specifies to start the management lock function.
stop - Specifies to stop the management lock function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To start management lock:

```
DWS-3160-24PC:admin# cfm lock md op-domain ma op-ma mepid 1 remote_mepid 2
action start
Command: cfm lock md op-domain ma op-ma mepid 1 remote_mepid 2 action start

Success.

DWS-3160-24PC:admin#
```

20-4 config cfm ccm_fwd

Description

This command is used to configure the CCM PDUs forwarding mode.

Format

config cfm ccm_fwd [software | hardware]

Parameters

software - Specifies that the CCM PDUs will be forwarded using the software mode.

hardware - Specifies that the CCM PDUs will be forwarded using the hardware mode.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the CCM PDUs forwarding mode:

```
DWS-3160-24PC:admin# config cfm ccm_fwd_mode hardware
Command: config cfm ccm_fwd_mode hardware

Success.

DWS-3160-24PC:admin#
```

20-5 show cfm ccm_fwd

Description

This command is used to display the CCM PDUs forwarding mode.

Format

show cfm ccm_fwd

Parameters

None.

Restrictions

None.

Example

To display the CCM PDUs forwarding mode:

```
DWS-3160-24PC:admin#show cfm ccm_fwd
Command: show cfm ccm_fwd

CFM CCM PDUs forwarding mode: Software

DWS-3160-24PC:admin#
```

Chapter 21 CPU Interface Filtering Command List

create cpu access_profile profile_id <value 1-5> [ethernet {vlan | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}]

delete cpu access_profile [profile_id <value 1-5> | all]

config cpu access_profile profile_id <value 1-5> [add access_id [auto_assign | <value 1-100>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] | source_ip <ipaddr> | 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 [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}]} | packet_content {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>} | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}] port [<portlist> | all] [permit | deny] {time_range <range_name 32>} | delete access_id <value 1-100>]

enable cpu_interface_filtering

disable cpu_interface_filtering

show cpu access_profile {profile_id <value 1-5>}

21-1 create cpu access_profile

Description

This command is used to create CPU access list rules.

Format

create cpu access_profile profile_id <value 1-5> [ethernet {vlan | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31

<hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}]

Parameters

profile_id - Specifies the profile ID used here.
  <value 1-5> - Enter the profile ID value here. This value must be between 1 and 5.

ethernet - Specifies that the profile type will be Ethernet.

vlan - (Optional) Specifies a VLAN mask.

source_mac - (Optional) Specifies the source MAC mask.
  <macmask> - Enter the source MAC mask here.

destination_mac - (Optional) Specifies the destination MAC mask.
  <macmask> - Enter the destination MAC mask here.

802.1p - (Optional) Specifies 802.1p priority tag mask.

ethernet_type - (Optional) Specifies the ethernet type mask.

ip - Specifies that the profile type will be IP.

vlan - (Optional) Specifies a VLAN mask.

source_ip_mask - (Optional) Specifies an IP source subnet mask.
  <netmask> - Enter the IP source subnet mask here.

destination_ip_mask - Specifies an IP destination subnet mask.
  <netmask> - Enter the IP destination subnet mask here.

dscp - Specifies the DSCP mask.

icmp - Specifies that the rule applies to ICMP traffic.
  type - (Optional) Specifies that the rule applies to ICMP type traffic.
  code - (Optional) Specifies that the rule applies to ICMP code traffic.

igmp - Specifies that the rule applies to IGMP traffic.
  type - (Optional) Specifies that the rule applies to IGMP type traffic.

tcp - Specifies that the rule applies to TCP traffic.
  src_port_mask - (Optional) Specifies the TCP source port mask.
    <hex 0x0-0xffff> - Enter the source TCP port mask here.
  dst_port_mask - (Optional) Specifies the TCP destination port mask.
    <hex 0x0-0xffff> - Enter the destination TCP port mask here.

flag_mask - (Optional) Specifies the TCP flag field mask.
  all - Specifies that the TCP flag field mask will be set to all.
  urg - Specifies that the TCP flag field mask will be set to urg.
  ack - Specifies that the TCP flag field mask will be set to ack.
  psh - Specifies that the TCP flag field mask will be set to psh.
  rst - Specifies that the TCP flag field mask will be set to rst.
  syn - Specifies that the TCP flag field mask will be set to syn.
  fin - Specifies that the TCP flag field mask will be set to fin.

udp - Specifies that the rule applies to UDP traffic.
  src_port_mask - (Optional) Specifies the UDP source port mask.
    <hex 0x0-0xffff> - Enter the source UDP port mask here.
  dst_port_mask - (Optional) Specifies the UDP destination port mask.
    <hex 0x0-0xffff> - Enter the destination UDP port mask here.

protocod_id_mask - Specifies that the rule applies to the IP protocol ID traffic.
  <0x0-0xff> - Enter the IP protocol ID mask here.

user_define_mask - (Optional) Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header length is 20 bytes.
  <hex 0x0-0xffffffff> - Enter the user-defined IP protocol ID mask here.

packet_content_mask - Specifies the frame content mask, there are 5 offsets in maximum could be configure. Each offset presents 16 bytes, the range of mask of frame is 80 bytes (5 offsets) in the first eighty bytes of frame.
  offset_0-15 - (Optional) Specifies that the mask pattern offset of the frame will be between 0 and 15.

<hex 0x0-0xffffffff> - Enter the mask pattern offset of the frame between 0 and 15 here. **offset_16-31** - (Optional) Specifies that the mask pattern offset of the frame will be between 16 and 31. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 16 and 31 here. **offset_32-47** - (Optional) Specifies that the mask pattern offset of the frame will be between 32 and 47. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 32 and 47 here. **offset_48-63** - (Optional) Specifies that the mask pattern offset of the frame will be between 48 and 63. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 48 and 63 here. **offset_64-79** - (Optional) Specifies that the mask pattern offset of the frame will be between 64 and 79. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 64 and 79 here.
ipv6 - Specifies IPv6 filtering mask.
class - (Optional) Specifies the IPv6 class.
flowlabel - (Optional) Specifies the IPv6 flowlabel.
source_ipv6_mask - (Optional) Specifies an IPv6 source subnet mask. **<ipv6mask>** - Enter the IPv6 source subnet mask here.
destination_ipv6_mask - (Optional) Specifies an IPv6 destination subnet mask. **<ipv6mask>** - Enter the IPv6 destination subnet mask here.
tcp - (Optional) Specifies that the rule applies to TCP traffic. **src_port_mask** - Specifies an IPv6 Layer 4 TCP source port mask. **<hex 0x0-0xffff>** - Enter the TCP source port mask value here. **des_port_mask** - Specifies an IPv6 Layer 4 TCP destination port mask. **<hex 0x0-0xffff>** - Enter the TCP destination port mask value here.
udp - (Optional) Specifies that the rule applies to UDP traffic. **src_port_mask** - Specifies the UDP source port mask. **<hex 0x0-0xffff>** - Enter the UDP source port mask value here. **dst_port_mask** - Specifies the UDP destination port mask. **<hex 0x0-0xffff>** - Enter the UDP destination port mask value here.
icmp - (Optional) Specifies a mask for ICMP filtering. **type** - Specifies the inclusion of the ICMP type field in the mask. **code** - Specifies the inclusion of the ICMP code field in the mask.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create CPU access list rules:

```
DWS-3160-24PC:admin#create cpu access_profile profile_id 1 ethernet vlan
source_mac 00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p
ethernet_type
Command: create cpu access_profile profile_id 1 ethernet vlan source_mac 00-00-
00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p ethernet_type

Success.

DWS-3160-24PC:admin#create cpu access_profile profile_id 2 ip vlan
source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type code
Command: create cpu access_profile profile_id 2 ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code

Success.

DWS-3160-24PC:admin#
```

21-2 delete cpu access_profile

Description

This command is used to delete CPU access list rules.

Format

delete cpu access_profile [profile_id <value 1-5> | all]

Parameters

profile_id - Specifies the index of access list profile.
  <value 1-5> - Enter the profile ID value here. This value must be between 1 and 5.
  all – Specifies that all the access list profiles will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete CPU access list rules:

```
DWS-3160-24PC:admin# delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DWS-3160-24PC:admin#
```

21-3 config cpu access_profile

Description

This command is used to configure CPU access list entry.

Format

config cpu access_profile profile_id <value 1-5> [add access_id [auto_assign | <value 1-100>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] | source_ip <ipaddr> | 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 [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}]} | packet_content {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>} | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}] port [<portlist> | all] [permit | deny] {time_range <range_name 32>} | delete access_id <value 1-100>]

Parameters

profile_id - Specifies the index of access list profile.
<value 1-5> - Enter the profile ID value here. This value must be between 1 and 5.

access_id - Specifies the index of access list entry. The range of this value is 1-100.
<value 1-100> - Enter the access ID here. This value must be between 1 and 100.

ethernet - Specifies that the profile type will be Ethernet.

vlan - (Optional) Specifies the VLAN name used.
<vlan_name 32> - Enter the name of the VLAN here. This name can be up to 32 characters long.

vlan_id - (Optional) Specifies the VLAN ID used.
<vid> - Enter the VLAN ID used here.
mask - (Optional) Specifies the mask used.
<hex 0x0-0x0fff> - Specifies the mask used.

source_mac - (Optional) Specifies the source MAC address.
<macaddr> - Enter the source MAC address used for this configuration here.
mask - (Optional) Specifies the mask used.
<hex 0x0-0x0fff> - Specifies the mask used.

destination_mac - (Optional) Specifies the destination MAC.
<macaddr> - Enter the destination MAC address used for this configuration here.
mask - (Optional) Specifies the mask used.
<hex 0x0-0x0fff> - Specifies the mask used.

802.1p - (Optional) Specifies the value of 802.1p priority tag.
<value 0-7> - Enter the 802.1p priority tag value here. This value must be between 0 and 7.

ethernet_type - (Optional) Specifies the Ethernet type.
<hex 0x0-0xffff> - Enter the Ethernet type value here.

ip - Specifies that the profile type will be IP.

vlan - (Optional) Specifies the VLAN name used.
<vlan_name 32> - Enter the name of the VLAN here. This name can be up to 32 characters long.

vlan_id - (Optional) Specifies the VLAN ID used.
<vid> - Enter the VLAN ID used here.

source_ip - (Optional) Specifies an IP source address.
<ipaddr> - Enter the source IP address used for this configuration here.
mask - (Optional) Specifies the mask.
<netmask> - Specifies the mask.

destination_ip - (Optional) Specifies an IP destination address.
<ipaddr> - Enter the destination IP address used for this configuration here.
mask - (Optional) Specifies the mask.
<netmask> - Specifies the mask.

dscp - (Optional) Specifies the value of DSCP, the value can be configured 0 to 63.
<value> - Enter the DSCP value used here.

icmp - (Optional) Specifies that the rule applies to ICMP traffic.
type - Specifies that the rule applies to the value of ICMP type traffic.
<value 0-255> - Enter the ICMP type value here. This value must be between 0 and 255.
code - Specifies that the rule applies to the value of ICMP code traffic.
<value 0-255> - Enter the ICMP code value here. This value must be between 0 and 255.

igmp - (Optional) Specifies that the rule applies to IGMP traffic.
type - Specifies that the rule applies to the value of IGMP type traffic.
<value 0-255> - Enter the IGMP type value here. This value must be between 0 and 255.

tcp - (Optional) Specifies that the rule applies to TCP traffic.
src_port - Specifies that the rule applies the range of TCP source port.
<value 0-65535> - Enter the source port value here. This value must be between 0 and 65535.
mask - (Optional) Specifies the mask.
<hex 0x0-0xffff> - Specifies the mask.
dst_port - Specifies the range of TCP destination port range.
<value 0-65535> - Enter the destination port value here. This value must be between 0 and 65535.
mask - (Optional) Specifies the mask.
<hex 0x0-0xffff> - Specifies the mask.

flag - (Optional) Specifies the TCP flag fields .
all - Specifies that the TCP flag field mask will be set to all.
urg - Specifies that the TCP flag field mask will be set to urg.
ack - Specifies that the TCP flag field mask will be set to ack.
psh - Specifies that the TCP flag field mask will be set to psh.
rst - Specifies that the TCP flag field mask will be set to rst.
syn - Specifies that the TCP flag field mask will be set to syn.
fin - Specifies that the TCP flag field mask will be set to fin.

udp - Specifies that the rule applies to UDP traffic.
src_port - (Optional) Specifies the range of UDP source port range.
<value 0-65535> - Enter the source port value here. This value must be between 0 and 65535.
mask - (Optional) Specifies the mask.
<hex 0x0-0xffff> - Specifies the mask.
dst_port - (Optional) Specifies the range of UDP destination port mask.
<value 0-65535> - Enter the destination port value here. This value must be between 0 and 65535.
mask - (Optional) Specifies the mask.
<hex 0x0-0xffff> - Specifies the mask.

protocol_id - Specifies that the rule applies to the value of IP protocol ID traffic.
<value 0-255> - Enter the protocol ID value here. This value must be between 0 and 255.

user_define - (Optional) Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header length is 20 bytes.
<hex 0x0-0xffffffff> - Enter the user-defined IP protocol ID mask here.
mask - (Optional) Specifies the mask.
<hex 0x0-0xffffffff> - Specifies the mask.

packet_content - Specifies the frame content pattern, there are 5 offsets in maximum could be configure. Each offset presents 16 bytes, the range of content of frame is 80 bytes(5 offsets) in the first eighty bytes of frame.
offset_0-15 - (Optional) Specifies that the mask pattern offset of the frame will be between 0 and 15.
<hex 0x0-0xffffffff> - Enter the mask pattern offset of the frame between 0 and 15 here.
offset_16-31 - (Optional) Specifies that the mask pattern offset of the frame will be between 16 and 31.

<hex 0x0-0xffffffff> - Enter the mask pattern offset of the frame between 16 and 31 here.
offset_32-47 - (Optional) Specifies that the mask pattern offset of the frame will be between 32 and 47.
<hex 0x0-0xffffffff> - Enter the mask pattern offset of the frame between 32 and 47 here.
offset_48-63 - (Optional) Specifies that the mask pattern offset of the frame will be between 48 and 63.
<hex 0x0-0xffffffff> - Enter the mask pattern offset of the frame between 48 and 63 here.
offset_64-79 - (Optional) Specifies that the mask pattern offset of the frame will be between 64 and 79.
<hex 0x0-0xffffffff> - Enter the mask pattern offset of the frame between 64 and 79 here.

ipv6 - Specifies the rule applies to IPv6 fields.

class - (Optional) Specifies the value of IPv6 class.
<value 0-255> - Enter the IPv6 class value here. This value must be between 0 and 255.

flowlabel - (Optional) Specifies the value of IPv6 flowlabel.
<hex 0x0-0xffff> - Enter the IPv6 flowlabel here.

source_ipv6 - (Optional) Specifies the value of IPv6 source address.
<ipv6addr> - Enter the IPv6 source address used for this configuration here.
mask - (Optional) Specifies the mask.
<ipv6mask> - Specifies the mask.

destination_ipv6 - (Optional) Specifies the value of IPv6 destination address.
<ipv6addr> - Enter the IPv6 destination address used for this configuration here.
mask - (Optional) Specifies the mask.
<ipv6mask> - Specifies the mask.

tcp - (Optional) Specifies to configure the TCP parameters.
src_port - Specifies the value of the IPv6 Layer 4 TCP source port.
<value 0-65535> - Enter the TCP source port value here. This value must be between 0 and 65535.
mask - Specifies an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the TCP source port mask value here.
dst_port - (Optional) Specifies the value of the IPv6 Layer 4 TCP destination port.
<value 0-65535> - Enter the TCP destination port value here. This value must be between 0 and 65535.
mask - Specifies an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the TCP destination port mask value here.

udp - (Optional) Specifies to configure the UDP parameters.
src_port - Specifies the value of the IPv6 Layer 4 UDP source port.
<value 0-65535> - Enter the UDP source port value here. This value must be between 0 and 65535.
mask - Specifies an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the UDP source port mask value here.
dst_port - Specifies the value of the IPv6 Layer 4 UDP destination port.
<value 0-65535> - Enter the UDP destination port value here. This value must be between 0 and 65535.
mask - Specifies an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the UDP destination port mask value here.

icmp - (Optional) Specifies to configure the ICMP parameters used.
type - Specifies that the rule applies to the value of ICMP type traffic.
<value 0-255> - Enter the ICMP type traffic value here. This value must be between 0 and 255.
code - Specifies that the rule applies to the value of ICMP code traffic.
<value 0-255> - Enter the ICMP code traffic value here. This value must be between 0 and 255.

port - Specifies the list of ports to be included in this configuration.
<portlist> - Enter a list of ports used for the configuration here.
all - Specifies that all the ports will be used for this configuration.

permit - Specifies the packets that match the access profile are permit by the Switch.
deny - Specifies the packets that match the access profile are filtered by the Switch.

time_range - (Optional) Specifies name of this time range entry.
<range_name> - Enter the time range here.

delete - Specifies to delete a rule from the profile ID entered.

access_id - Specifies the index of access list entry. The range of this value is 1-100.
  <value 1-100> - Enter the access ID here. This value must be between 1 and 100.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure CPU access list entry:

```
DWS-3160-24PC:admin# config cpu access_profile profile_id 1 add access_id 1 ip
vlan default source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11
code 32 port 1 deny
Command: config cpu access_profile profile_id 1 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port 1
deny


Success.


DWS-3160-24PC:admin#
```

21-4 enable cpu interface filtering

Description

This command is used to enable CPU interface filtering control.

Format

enable cpu_interface_filtering

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable cpu_interface_filtering:

```
DWS-3160-24PC:admin# enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DWS-3160-24PC:admin#
```

21-5 disable cpu interface filtering

Description

This command is used to disable CPU interface filtering control.

Format

disable cpu_interface_filtering

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable cpu_interface_filtering:

```
DWS-3160-24PC:admin# disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DWS-3160-24PC:admin#
```

21-6 show cpu access_profile

Description

This command is used to display current access list table.

Format

show cpu access_profile {profile_id <value 1-5>}

Parameters

profile_id - (Optional) Specifies the index of access list profile.
<value 1-5> - Enter the profile ID used here. This value must be between 1 and 5.

Restrictions

None.

Example

To display current cpu access list table:

```
DWS-3160-24PC:admin# show cpu access_profile
Command: show cpu access_profile

CPU Interface Filtering State: Disabled

CPU Interface Access Profile Table

Total Unused Rule Entries : 497
Total Used Rule Entries   : 3

==============================================================================
Profile ID: 1     Type: IPv6

MASK on
    Source IPv6 Addr : FFFF:FFFF:FFFF::

Unused Rule Entries: 99
------------------------------------------------------------------------------
Rule ID : 1       Ports: 20

Match on
    Source IPv6 : 2103:16:16::

Action:
    Deny

==============================================================================

==============================================================================
Profile ID: 2     Type: IPv4

MASK on
    Source IP   : 255.255.0.0

Unused Rule Entries: 99
------------------------------------------------------------------------------
Rule ID : 1       Ports: 20

Match on
    Source IP   : 172.18.0.0

Action:
    Deny

==============================================================================

==============================================================================
Profile ID: 3     Type: Ethernet

MASK on
    Source MAC      : FF-FF-FF-FF-FF-FF
```

```
Unused Rule Entries: 99
------------------------------------------------------------------------------
Rule ID : 1       Ports: 1-24

Match on
    Source MAC      : 00-00-22-B0-61-51

Action:
    Deny

==============================================================================

==============================================================================
Profile ID: 4     Type: User Defined

MASK on
    Offset  0-15 : 0xFFF000FF 0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF
    Offset 16-31 : 0xFFFFFFFF 0xFFFFFFFF 0xFF00FFFF 0xFFFFFFFF
    Offset 32-47 : 0xFFFFFFFF 0xFFFFFFFF 0x000FFFFF 0xFFFFFFFF
    Offset 48-63 : 0xFFFFFFFF 0xFFFFFFFF 0xFFFFF000 0xFFFFFFFF
    Offset 64-79 : 0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF 0xFFFFF000

Unused Rule Entries: 100
==============================================================================

DWS-3160-24PC:admin#
```

Chapter 22 Debug Software Command List

debug error_log [dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]

debug buffer [utilization | dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]

debug output [module <module_list> | all] [buffer | console]

debug config error_reboot [enable | disable]

debug config state [enable | disable]

debug show arpunresolved_list

debug show error_reboot state

debug show status {module <module_list>}

debug address_binding [event | dhcp | all] state [enable | disable]

no debug address_binding

debug stp config ports [<portlist> | all] [event | bpdu | state_machine | all] state [disable | brief | detail]

debug stp show information

debug stp show flag {ports <portlist>}

debug stp show counter {ports [<portlist> | all]}

debug stp clear counter [ports <portlist> | all]

debug stp state [enable | disable]

22-1 debug error_log

Description

This command is use to dump, clear or upload the software error log to a TFTP server.

Format

debug error_log [dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]

Parameters

dump - Display the debug message of the debug log.

clear - Clear the debug log.

upload_toTFTP - Upload the debug log to a TFTP server specified by IP address.
<ipaddr> - Specifies the IPv4 address of the TFTP server.
<path_filename 64> - The pathname specifies the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This value can be up to 64 characters long.

Restrictions

Only Administrators can issue this command.

Example

To dump the error log:

```
DWS-3160-24PC:admin# debug error_log dump
Command: debug error_log dump

**************************************************************************
# debug log: 1
# level: fatal
# clock: 10000ms
# time : 2009/03/11 13:00:00

====================== SOFTWARE FATAL ERROR =======================
Invalid mutex handle : 806D6480

Current TASK : bcmARL.0

------------------------- TASK STACKTRACE ------------------------
->802ACE98
->8018C814
->8028FF44
->8028352C
->801D703C
->8013B8A4
->802AE754
->802A5E0C
```

To clear the error log:

```
DWS-3160-24PC:admin# debug error_log clear
Command: debug error_log clear

Success.

DWS-3160-24PC:admin#
```

To upload the error log to TFTP server:

```
DWS-3160-24PC:admin# debug error_log upload_toTFTP 10.0.0.90 debug-log.txt
Command: debug error_log upload_toTFTP 10.0.0.90 debug-log.txt

Connecting to server................Done.
Upload error log  ..................Done.

DWS-3160-24PC:admin#
```

22-2 debug buffer

Description

This command is use to display the debug buffer’s state, or dump, clear, or upload the debug buffer to a TFTP server.

Format

debug buffer [utilization | dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]

Parameters

utilization - Display the debug buffer's state.

dump - Display the debug message in the debug buffer.

clear - Clear the debug buffer.

upload_toTFTP - Upload the debug buffer to a TFTP server specified by IP address.
<ipaddr> - Specifies the IPv4 address of the TFTP server.
<path_filename 64> - The pathname specifies the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This value can be up to 64 characters long.

Restrictions

Only Administrators can issue this command.

Example

To display the debug buffer's state:

```
DWS-3160-24PC:admin# debug buffer utilization
Command: debug buffer utilization

Allocate from       :      System memory pool
Total size          :      2 MB
Utilization rate    :      30%

DWS-3160-24PC:admin#
```

To clear the debug buffer:

```
DWS-3160-24PC:admin# debug buffer clear
Command: debug buffer clear

Success.

DWS-3160-24PC:admin#
```

To upload the messages stored in debug buffer to TFTP server:

```
DWS-3160-24PC:admin# debug buffer upload_toTFTP 10.0.0.90 debugcontent.txt
Command: debug buffer upload_toTFTP 10.0.0.90 debugcontent.txt

Connecting to server................... Done.
Upload debug file   ................... Done.

DWS-3160-24PC:admin#
```

22-3 debug output

Description

This command is use to set a specified module’s debug message output to debug buffer or local console. If the user uses the command in a TELNET session, the error message also is output to the local console.

Format

debug output [module <module_list> | all] [buffer | console]

Parameters

module - Specifies the module list.
  <module_list> - Enter the module list here.
  all - Control output method of all modules.

buffer - Direct the debug message of the module output to debug buffer(default).

console - Direct the debug message of the module output to local console.

Restrictions

Only Administrators can issue this command.

Example

To set all module debug message outputs to local console:

```
DWS-3160-24PC:admin# debug output all console
Command: debug output all console

Success.

DWS-3160-24PC:admin#
```

22-4 debug config error_reboot

Description

This command is used to set if the Switch needs to be rebooted when a fatal error occurs. When the error occurs, the watchdog timer will be disabled by the system first, and then all debug information will be saved in NVRAM. If the error_reboot is enabled, the watchdog shall be enabled after all information is stored into NVRAM.

Format

debug config error_reboot [enable | disable]

Parameters

enable – If enabled, the Switch will reboot when a fatal error happens.
disable – If disabled the Switch will not reboot when a fatal error happens, system will hang-up for debug and enter the debug shell mode for debug.

Restrictions

Only Administrators can issue this command.

Example

To set the Switch to not need a reboot when a fatal error occurs:

```
DWS-3160-24PC:admin# debug config error_reboot disable
Command: debug config error_reboot disable

Success.

DWS-3160-24PC:admin#
```

22-5 debug config state

Description

Use the command to set the state of the debug.

Format

debug config state [enable | disable]

Parameters

enable - Enable the debug state.
disable - Disable the debug state.

Restrictions

Only Administrators can issue this command.

Example

To set the debug state to disabled:

```
DWS-3160-24PC:admin# debug config state disable
Command: debug config state disable

Success.

DWS-3160-24PC:admin#
```

22-6 debug show arpunresolved_list

Description

This command is used to debug the ARP unresolved list.

Format

debug show arpunresolved_list

Parameters

None.

Restrictions

None.

Example

To debug the ARP unresolved list:

```
DWS-3160-24PC:admin#debug show arpunresolved_list
Command: debug show arpunresolved_list

Unresolved ARP list

IP Address       last_send  send_int  send_cnt  flag
---------------  ---------  --------  --------  ----


DWS-3160-24PC:admin#
```

22-7 debug show error_reboot state

Description

This command is used to display ‘show error reboot’ status.

Format

debug show error_reboot state

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display ‘show error reboot’ status:

```
DWS-3160-24PC:admin#debug show error_reboot state
Command: debug show error_reboot state

Error Reboot: Enabled

DWS-3160-24PC:admin#
```

22-8 debug show status

Description

This command is used to display the debug handler’s state and to specify the module’s debug status. If the input module list is empty, the states of all the registered modules, that support the debug module, will be displayed.

Format

debug show status {module <module_list>}

Parameters

module – (Optional) Specifies the module list.
<module_list> - Enter the module list here.

Restrictions

Only Administrators can issue this command.

Example

To display the specified module’s debug state:

```
DWS-3160-24PC:admin#debug show status module MSTP
Command: debug show status module MSTP

Debug Global State  : Enabled

MSTP                : Disabled

DWS-3160-24PC:admin#
```

To display the debug state:

```
DWS-3160-24PC:admin#debug show status
Command: debug show status

Debug Global State  : Disabled

MSTP                : Disabled
IMPB                : Disabled
VRRP                : Disabled
ERPS                : Disabled
WLAN                : Disabled
CP                  : Disabled

DWS-3160-24PC:admin#
```

22-9 debug address_binding

Description

This command is used to start the IMPB debug when the IMPB module receives an ARP/IP packet or a DHCP packet.

Format

debug address_binding [event | dhcp | all] state [enable | disable]

Parameters

event - To print out the debug messages when IMPB module receives ARP/IP packets. **dhcp** - To print out the debug messages when the IMPB module receives the DHCP packets. **all** - Print out all debug messages.
state - This parameter configures the IMPB debug state to be enabled or disabled. **enable** - Specifies that the state will be enabled. **disable** - Specifies that the state will be disabled.

Restrictions

Only Administrators can issue this command.

Example

To print out all debug IMPB messages:

```
DWS-3160-24PC:admin# debug address_binding all state enable
Command: debug address_binding all state enable

Success.

DWS-3160-24PC:admin#
```

22-10 no debug address_binding

Description

This command is used to stop the IMPB debug starting when the IMPB module receives an ARP/IP packet or a DHCP packet.

Format

no debug address_binding

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To stop IMPB debug: starting when the IMPB module receives an ARP/IP or DHCP packet:

```
DWS-3160-24PC:admin# no debug address_binding
Command: no debug address_binding

Success.

DWS-3160-24PC:admin#
```

22-11 debug stp config ports

Description

This command used to configure per-port STP debug level on the specified ports.

Format

debug stp config ports [<portlist> | all] [event | bpdu | state_machine | all] state [disable | brief | detail]

Parameters

ports - Specifies the STP port range to debug. **<portlist>** - Enter the list of port used for this configuration here. **all** - Specifies to debug all ports on the Switch.
event - Debug the external operation and event processing. **bpdu** - Debug the BPDU's that have been received and transmitted. **state_machine** - Debug the state change of the STP state machine. **all** - Debug all of the above.
state - Specifies the state of the debug mechanism. **disable** - Disables the debug mechanism. **brief -** Sets the debug level to brief.

detail - Sets the debug level to detail.

Restrictions

Only Administrators can issue this command.

Example

To configure all STP debug flags to brief level on all ports:

```
DWS-3160-24PC:admin# debug stp config ports all state brief
Command: debug stp config ports all state brief

 Warning: only support local device.

Success.

DWS-3160-24PC:admin#
```

22-12 debug stp show information

Description

This command used to display STP detailed information, such as the hardware tables, the STP state machine, etc.

Format

debug stp show information

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display STP debug information:

```
DWS-3160-24PC:admin# debug stp show information
Command: debug stp show information

Warning: only support local device.
Spanning Tree Debug Information:
----------------------------------------
Port Status In Hardware Table:
Instance 0:
Port 1 : FOR  Port 2 : FOR  Port 3 : FOR  Port 4 : FOR  Port 5 : FOR  Port 6 :
FOR
```

```
Port 7 : FOR  Port 8 : FOR  Port 9 : FOR  Port 10: FOR  Port 11: FOR  Port 12:
FOR
Port 13: FOR  Port 14: FOR  Port 15: FOR  Port 16: FOR  Port 17: FOR  Port 18:
FOR
Port 19: FOR  Port 20: FOR  Port 21: FOR  Port 22: FOR  Port 23: FOR  Port 24:
FOR
--------------------------------------
Root Priority And Times:
Instance 0:
 Designated Root Bridge : 32768/00-01-70-33-21-02
 External Root Cost     : 0
 Regional Root Bridge   : 32768/00-01-70-33-21-02
 Internal Root Cost     : 0
 Designated Bridge      : 32768/00-01-70-33-21-02
 Designated Port        : 0
 Message Age            : 0
 Max Age                : 20
 Forward Delay          : 15
 Hello Time             : 2
--------------------------------------
Designated Priority And Times:
 Instance 0:
--------------------------------------
Port Priority And Times:
Instance 0:

DWS-3160-24PC:admin#
```

22-13 debug stp show flag

Description

This command used to display the STP debug level on specified ports.

Format

debug stp show flag {ports <portlist>}

Parameters

ports - (Optional) Specifies the STP ports to display.
    <portlist> - (Optional) Enter the list of port used for this configuration here.

If no parameter is specified, all ports on the Switch will be displayed.

Restrictions

Only Administrators can issue this command.

Example

To display the debug STP levels on all ports:

```
DWS-3160-24PC:admin#debug stp show flag
```

```
Command: debug stp show flag

Warning: only support local device.

Global State: Enabled

Port Index       Event Flag       BPDU Flag       State Machine Flag
----------------------------------------------------------
 1             Brief            Brief           Brief
 2             Brief            Brief           Brief
 3             Brief            Brief           Brief
 4             Brief            Brief           Brief
 5             Brief            Brief           Brief
 6             Brief            Brief           Brief
 7             Brief            Brief           Brief
 8             Brief            Brief           Brief
 9             Brief            Brief           Brief
 10            Brief            Brief           Brief
 11            Brief            Brief           Brief
 12            Brief            Brief           Brief
 13            Brief            Brief           Brief
 14            Brief            Brief           Brief
 15            Brief            Brief           Brief
 16            Brief            Brief           Brief
 17            Brief            Brief           Brief
 18            Brief            Brief           Brief
 19            Brief            Brief           Brief
 20            Brief            Brief           Brief
 21            Brief            Brief           Brief
 22            Brief            Brief           Brief
 23            Brief            Brief           Brief
 24            Brief            Brief           Brief

DWS-3160-24PC:admin#
```

22-14 debug stp show counter

Description

This command used to display the STP counters.

Format

debug stp show counter {ports [<portlist> | all]}

Parameters

ports - (Optional) Specifies the STP ports for display.
 <portlist> - Enter the list of port used for this configuration here.
 all - Display all port's counters.

If no parameter is specified, display the global counters.

Restrictions

Only Administrators can issue this command.

Example

To display the STP counters for port 9:

```
DWS-3160-24PC:admin# debug stp show counter ports 9
Command: debug stp show counter ports 9

STP Counters
--------------------------------------
 Port 9  :
  Receive:                                   Transmit:
  Total STP Packets         : 0              Total STP Packets  : 0
  Configuration BPDU        : 0              Configuration BPDU : 0
  TCN BPDU                  : 0              TCN BPDU           : 0
  RSTP TC-Flag              : 0              RSTP TC-Flag       : 0
  RST BPDU                  : 0              RST BPDU           : 0

  Discard:
  Total Discarded BPDU      : 0
  Global STP Disabled       : 0
  Port STP Disabled         : 0
  Invalid packet Format     : 0
  Invalid Protocol          : 0
  Configuration BPDU Length : 0
  TCN BPDU Length           : 0
  RST BPDU Length           : 0
  Invalid Type              : 0
  Invalid Timers            : 0

DWS-3160-24PC:admin#
```

22-15 debug stp clear counter

Description

This command used to clear the STP counters.

Format

debug stp clear counter [ports <portlist> | all]

Parameters

ports - Specifies the port range.
  <portlist> - Enter the list of port used for this configuration here.
  all - Clears all port counters.

Restrictions

Only Administrators can issue this command.

Example

To clear all STP counters on the Switch:

```
DWS-3160-24PC:admin# debug stp clear counter ports all
Command: debug stp clear counter ports all

 Warning: only support local device.

Success.

DWS-3160-24PC:admin#
```

22-16 debug stp state

Description

This command is used to enable or disable the STP debug state.

Format

debug stp state [enable | disable]

Parameters

state - Specifies the STP debug state.
  enable - Enable the STP debug state.
  disable - Disable the STP debug state.

Restrictions

Only Administrators can issue this command.

Example

To configure the STP debug state to enable, and then disable the STP debug state:

```
DWS-3160-24PC:admin# debug stp state enable
Command: debug stp state enable

Success.

DWS-3160-24PC:admin# debug stp state disable
Command: debug stp state disable

Success.

DWS-3160-24PC:admin#
```

Chapter 23 DHCP Local Relay Command List

config dhcp_local_relay vlan <vlan_name 32> state [enable | disable]
config dhcp_local_relay vlan vlanid <vlan_id> state [enable | disable]
enable dhcp_local_relay
disable dhcp_local_relay
show dhcp_local_relay

23-1 config dhcp_local_relay

Description

This command is used to enable or disable DHCP local relay function for specified VLAN name.

When DHCP local relay is enabled for the VLAN, the DHCP packet will be relayed in broadcast way without change of the source MAC address and gateway address. DHCP option 82 will be automatically added.

Format

config dhcp_local_relay vlan <vlan_name 32> state [enable | disable]

Parameters

vlan - Specifies the VLAN name that the DHCP local relay function will be enabled. **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long.
state - Enable or disable DHCP local relay for specified vlan. **enable** - Specifies that the DHCP local relay function will be enabled. **disable** - Specifies that the DHCP local relay function will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable DHCP local relay for default VLAN:

```
DWS-3160-24PC:admin# config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable

Success.

DWS-3160-24PC:admin#
```

23-2 config dhcp_local_relay vlan vlanid

Description

This command is used to enable or disable DHCP local relay function for specified VLAN ID.

Format

config dhcp_local_relay vlan vlanid <vlan_id> state [enable | disable]

Parameters

vlanid - Specifies the VLAN ID that the DHCP local relay function will be enabled. **<vlan_id>** - Enter the VLAN ID used here.
state - Enable or disable DHCP local relay for specified vlan. **enable** - Specifies that the DHCP local relay function will be enabled. **disable** - Specifies that the DHCP local relay function will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable DHCP local relay for default VLAN:

```
DWS-3160-24PC:admin# config dhcp_local_relay vlan vlanid 1 state enable
Command: config dhcp_local_relay vlan vlanid 1 state enable

Success.

DWS-3160-24PC:admin#
```

23-3 enable dhcp_local_relay

Description

This command is use to globally enable the DHCP local relay function on the Switch.

Format

enable dhcp_local_relay

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the DHCP local relay function:

```
DWS-3160-24PC:admin# enable dhcp_local_relay
Command: enable dhcp_local_relay

Success.

DWS-3160-24PC:admin#
```

23-4 disable dhcp_local_relay

Description

This command is use to globally disable the DHCP local relay function on the Switch.

Format

disable dhcp_local_relay

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the DHCP local relay function:

```
DWS-3160-24PC:admin# disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.

DWS-3160-24PC:admin#
```

23-5 show dhcp_local_relay

Description

This command is use to display the current DHCP local relay configuration.

Format

show dhcp_local_relay

Parameters

None.

Restrictions

None.

Example

To display local dhcp relay status:

```
DWS-3160-24PC:admin#show dhcp_local_relay
Command: show dhcp_local_relay

DHCP/BOOTP Local Relay Status         : Enabled
DHCP/BOOTP Local Relay VID List       : 1

DWS-3160-24PC:admin#
```

Chapter 24 DHCP Relay Command List

config dhcp_relay {hops <int 1-16> | time <sec 0-65535>}

config dhcp_relay add ipif <ipif_name 12> <ipaddr>

config dhcp_relay delete ipif <ipif_name 12> <ipaddr>

config dhcp_relay option_82 check [enable | disable]

config dhcp_relay option_82 policy [replace | drop | keep]

config dhcp_relay option_82 remote_id [default | user_define <desc 32>]

config dhcp_relay option_82 state [enable | disable]

enable dhcp_relay

disable dhcp_relay

show dhcp_relay {ipif <ipif_name 12>}

config dhcp_relay option_60 state [enable | disable]

config dhcp_relay option_60 add string <multiword 255> relay <ipaddr> [exact-match | partial-match]

config dhcp_relay option_60 default [relay <ipaddr> | mode [drop | relay]]

config dhcp_relay option_60 delete [string <multiword 255> {relay <ipaddr>} | ipaddress <ipaddr> | all | default {<ipaddr>}]

show dhcp_relay option_60 {[string <multiword 255> | ipaddress <ipaddr> | default]}

config dhcp_relay option_61 state [enable | disable]

config dhcp_relay option_61 add [mac_address <macaddr> | string <desc_long 255>] [relay <ipaddr> | drop]

config dhcp_relay option_61 default [relay <ipaddr> | drop]

config dhcp_relay option_61 delete [mac_address <macaddr> | string <desc_long 255> | all]

show dhcp_relay option_61

24-1 config dhcp_relay

Description

This command is use to configure the DHCP relay feature of the Switch.

Format

config dhcp_relay {hops <int 1-16> | time <sec 0-65535>}

Parameters

hops - (Optional) Specifies the maximum number of relay hops that the DHCP/BOOTP packets can cross. The range is 1 to 16. The default value is 4. The DHCP packet will be dropped when the relay hop count in the received packet is equal to or greater than this setting.
<int 1-16> - Enter the maximum number of relay hops here. This value must be between 1 and 16.

time - (Optional) The time field in the DHCP packet must be equal to or greater than this setting to be relayed by the router. The default value is 0.
<sec 0-65535> - Enter the relay time here. This value must be between 0 and 65535 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DHCP relay hops and time parameters:

```
DWS-3160-24PC:admin# config dhcp_relay hops 4 time 2
Command: config dhcp_relay hops 4 time 2

Success.

DWS-3160-24PC:admin#
```

24-2 config dhcp_relay add

Description

This command is use to add an IP destination address to the Switch’s DHCP relay table. Used to configure a DHCP server for relay of packets.

Format

config dhcp_relay add ipif <ipif_name 12> <ipaddr>

Parameters

ipif_name - The name of the IP interface which contains the IP address below.

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

<ipaddr> - The DHCP/BOOTP server IP address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a DHCP/BOOTP server to the relay table:

```
DWS-3160-24PC:admin# config dhcp_relay add ipif System 10.43.21.12
Command: config dhcp_relay add ipif System 10.43.21.12

Success.

DWS-3160-24PC:admin#
```

24-3 config dhcp_relay delete

Description

This command is used to delete one of the IP destination addresses in the Switch’s relay table.

Format

config dhcp_relay delete ipif <ipif_name 12> <ipaddr>

Parameters

ipif - The name of the IP interface which contains the IP address below.
<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

<ipaddr> - The DHCP/BOOTP server IP address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a DHCP/BOOTP server to the relay table:

```
DWS-3160-24PC:admin# config dhcp_relay delete ipif System 10.43.21.12
Command: config dhcp_relay delete ipif System 10.43.21.12

Success.

DWS-3160-24PC:admin#
```

24-4 config dhcp_relay option_82 check

Description

This command is used to configure the checking of the DHCP Option 82 for the DHCP relay function.

Format

config dhcp_relay option_82 check [enable | disable]

Parameters

check - When the state is enabled, For packet come from client side, the packet should not have the option 82's field. If the packet has this option field, it will be dropped. The default setting is disabled.
enable - Specifies that checking will be enabled.
disable - Specifies that checking will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the checking of the DHCP Option 82 for the DHCP relay function:

```
DWS-3160-24PC:admin# config dhcp_relay option_82 check disable
Command: config dhcp_relay option_82 check disable

Success.

DWS-3160-24PC:admin#
```

24-5 config dhcp_relay option_82 policy

Description

This command is used to configure the policy of the DHCP Option 82 for the DHCP relay function.

Format

config dhcp_relay option_82 policy [replace | drop | keep]

Parameters

policy - Specifies the policy used. This option takes effect only when the check status is disabled. The default setting is set to 'replace'.

- **replace** - Replace the existing option 82 field in the packet. The Switch will use its own Option 82 value to replace the old Option 82 value in the packet.
- **drop** - Discard if the packet has the option 82 field. If the packet that comes from the client side contains and Option 82 value, then the packet will be dropped. If the packet that comes from the client side doesn't contain an Option 82 value, then insert its own Option 82 value into the packet.
- **keep** - Retain the existing option 82 field in the packet. If the packet, that comes from the client side, contains and Option 82 value, then keep the old Option 82 value. If the packet that comes from the client side doesn't contain an Option 82 value, then insert its own Option 82 value into the packet.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the policy of the DHCP Option 82 for the DHCP relay function:

```
DWS-3160-24PC:admin# config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DWS-3160-24PC:admin#
```

24-6 config dhcp_relay option_82 remote_id

Description

This command is used to configure the remote ID of the DHCP Option 82 for the DHCP relay function.

Format

config dhcp_relay option_82 remote_id [default | user_define <desc 32>]

Parameters

remote_id - Specifies the content in Remote ID sub option.

- **default** - Use Switch’s system MAC address as remote ID.
- **user_define** - Use user-defined string as remote ID. The space character is allowed in the string.
  - **<desc 32>** - Enter the user defined description here. This value can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the remote ID of the DHCP Option 82 for the DHCP relay function:

```
DWS-3160-24PC:admin#config dhcp_relay option_82 remote_id user_define "D-Link
Switch"
Command: config dhcp_relay option_82 remote_id user_define "D-Link Switch"

Success.

DWS-3160-24PC:admin#
```

24-7 config dhcp_relay option_82 state

Description

This command is used to configure the state of the DHCP Option 82 for the DHCP relay function.

Format

config dhcp_relay option_82 state [enable | disable]

Parameters

state - (Optional) When the state is enabled, the DHCP packet will be inserted with the option 82 field before being relayed to server. The DHCP packet will be processed based on the behavior defined in check and policy setting. When the state is disabled, the DHCP packet will be relayed directly to server without further check and processing on the packet. The default setting is disabled.

- **enable** - Specifies that the option 82 processing will be enabled.
- **disable** - Specifies that the option 82 processing will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the state of the DHCP Option 82 for the DHCP relay function:

```
DWS-3160-24PC:admin# config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DWS-3160-24PC:admin#
```

24-8 enable dhcp_relay

Description

This command is use to enable the DHCP relay function on the Switch.

Format

enable dhcp_relay

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the DHCP relay function.

```
DWS-3160-24PC:admin# enable dhcp_relay
Command: enable dhcp_relay

Success.

DWS-3160-24PC:admin#
```

24-9 disable dhcp_relay

Description

This command is use to disable the DHCP relay function on the Switch.

Format

disable dhcp_relay

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the DHCP relay function:

```
DWS-3160-24PC:admin# disable dhcp_relay
Command: disable dhcp_relay

Success.

DWS-3160-24PC:admin#
```

24-10 show dhcp_relay

Description

This command is use to display the current DHCP relay configuration.

Format

show dhcp_relay {ipif <ipif_name 12>}

Parameters

ipif - (Optional) Specifies the IP interface name.

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

If no parameter is specified , the system will display all DHCP relay configuration.

Restrictions

None.

Example

To display DHCP relay configuration:

```
DWS-3160-24PC:admin#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

DHCP/BOOTP Relay Status         : Enabled
DHCP/BOOTP Hops Count Limit     : 4
DHCP/BOOTP Relay Time Threshold : 2
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information Option 82 State  : Enabled
DHCP Relay Agent Information Option 82 Check  : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace
DHCP Relay Agent Information Option 82 Remote ID : "D-Link Switch"

Interface    Server 1        Server 2        Server 3        Server 4
------------ --------------- --------------- --------------- ---------------
System       10.90.90.254

DWS-3160-24PC:admin#
```

To display DHCP relay configuration:

```
DWS-3160-24PC:admin#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

DHCP/BOOTP Relay Status         : Enabled
DHCP/BOOTP Hops Count Limit     : 4
DHCP/BOOTP Relay Time Threshold : 2
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information Option 82 State  : Enabled
DHCP Relay Agent Information Option 82 Check  : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace
DHCP Relay Agent Information Option 82 Remote ID : "D-Link Switch"

Interface    Server 1        Server 2        Server 3        Server 4
------------ --------------- --------------- --------------- ---------------
System       10.90.90.254

DWS-3160-24PC:admin#
```

24-11 config dhcp_relay option_60

Description

This command is use to decides whether DHCP relay will process the DHCP Option 60 or not.

When Option 60 is enabled, if the packet does not have Option 60, then the relay servers cannot be determined based on Option 60. The relay servers will be determined based on either Option 61 or per IPIF configured servers.

If the relay servers are determined based on Option 60 or Option 61, then per IPIF configured servers will be ignored.

If the relay servers are not determined either by Option 60 or Option 61, then per IPIF configured servers will be used to determine the relay servers.

Format

config dhcp_relay option_60 state [enable | disable]

Parameters

state - Specifies that the DHCP relay function should use the Option 60 rule to relay the DHCP packets.
  enable - Specifies that the Option 60 rule will be enabled.
  disable - Specifies that the Option 60 rule will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the state of DHCP relay Option 60:

```
DWS-3160-24PC:admin# config dhcp_relay option_60 state enable
Command: config dhcp_relay option_60 state enable

Success

DWS-3160-24PC:admin#
```

24-12 config dhcp_relay option_60 add

Description

This command is use to configure the Option 60 relay rules.

NOTE: Different string values can be specified using the same relay server, and the same string can be specified with multiple relay servers. The system will relay the packet to all the matching servers.

Format

config dhcp_relay option_60 add string <multiword 255> relay <ipaddr> [exact-match | partial-match]

Parameters

string - Specifies the string used.
  <multiword 255> - Enter the string value here. This value can be up to 255 characters long.

relay - Specifies a relay server IP address.
  <ipaddr> - Enter the IP address used for this configuration here.

exact-match - The Option 60 string in the packet must full match with the specified string.
partial-match - The Option 60 string in the packet only need partial match with the specified string.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DHCP relay Option 60 option:

```
DWS-3160-24PC:admin# config dhcp_relay option_60 add string "abc" relay
10.90.90.1 exact-match
Command: config dhcp_relay option_60 add string "abc" relay 10.90.90.1 exact-
match

Success.

DWS-3160-24PC:admin#
```

24-13 config dhcp_relay option_60 default

Description

This command is use to configure the DHCP relay Option 60's default relay server setting. When there are no match servers found for the packet based on Option 60, the relay servers will be determined by the default relay server setting.

When there is no matching found for the packet, the relay servers will be determined based on the default relay servers.

When 'drop' is specified, the packet with no matching rules found will be dropped without further process.

If the setting is not set as 'drop', then the packet will be processed further based on Option 61. The final relay servers will be the union of Option 60 default relay servers and the relay servers determined by Option 61.

Format

config dhcp_relay option_60 default [relay <ipaddr> | mode [drop | relay]]

Parameters

relay - Specifies the IP address used for the DHCP relay forward function. **<ipaddr>** - Enter the IP address used for this configuration here.
mode - Specifies the DHCP relay Option 60 mode. **drop** - Specifies to drop the packet that has no matching Option 60 rules. **relay** - The packet will be relayed based on the relay rules.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DHCP relay Option 60 default drop option:

```
DWS-3160-24PC:admin#config dhcp_relay option_60 default mode drop
Command: config dhcp_relay option_60 default mode drop

Success.

DWS-3160-24PC:admin#
```

24-14 config dhcp_relay option_60 delete

Description

This command is use to delete a DHCP relay Option 60 entry.

Format

config dhcp_relay option_60 delete [string <multiword 255> {relay <ipaddr>} | ipaddress <ipaddr> | all | default {<ipaddr>}]

Parameters

string - Delete all the entries whose string is equal to the string of specified if ipaddress is not specified **<multiword 255>** - Enter the DHCP Option 60 string to be removed here. This value can be up to 255 characters long.
relay - (Optional) Delete one entry, whose string and IP address are equal to the string and IP address specified by the user. **<ipaddr>** - Enter the IP address used for this configuration here.
ipaddress - Delete all the entry whose ipaddress is equal to the specified ipaddress. **<ipaddr>** - Enter the IP address used for this configuration here. **all** - Delete all the entry. Default relay servers are excluded.
default - Delete the default relay ipaddress that is specified by the user. **<ipaddr>** - (Optional) Enter the IP address used for this configuration here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the DHCP relay Option 60 string called ‘abc’:

```
DWS-3160-24PC:admin# delete dhcp_relay option_60 string "abc" relay 10.90.90.1
Command: delete dhcp_relay option_60 string "abc" relay 10.90.90.1

Success

DWS-3160-24PC:admin#
```

24-15 show dhcp_relay option_60

Description

This command is use to display the DHCP relay Option 60 entry by the user specified.

Format

show dhcp_relay option_60 {[string <multiword 255> | ipaddress <ipaddr> | default]}

Parameters

string - (Optional) Display the entry which's string equal the string of specified.
  <multiword 255> - Enter the entry's string value here. This value can be up to 255 characters long.

ipaddress - (Optional) Display the entry whose IP address equal the specified ipaddress.
  <ipaddr> - Enter the IP address here.

default - (Optional) Display the default behavior of DHCP relay Option 60.

If no parameter is specified then all the DHCP Option 60 entries will be displayed.

Restrictions

None.

Example

To display DHCP Option 60 information:

```
DWS-3160-24PC:admin#show dhcp_relay option_60
Command: show dhcp_relay option_60

Default Processing Mode: Drop

Default Servers:

Matching Rules:

String                            Match Type              IP Address
-------                           ---------               ---------
abc                               Exact Match             10.90.90.1

Total Entries : 1

DWS-3160-24PC:admin#
```

24-16 config dhcp_relay option_61

Description

This command is use to decide whether the DHCP relay will process the DHCP Option 61 or not.

When Option 61 is enabled, if the packet does not have Option 61, then the relay servers cannot be determined based on Option 61.

If the relay servers are determined based on Option 60 or Option 61, then per IPIF configured servers will be ignored.

If the relay servers are not determined either by Option 60 or Option 61, then per IPIF configured servers will be used to determine the relay servers.

Format

config dhcp_relay option_61 state [enable | disable]

Parameters

state - Specifies whether the DHCP relay Option 61 is enabled or disabled.
 enable - Enables the function DHCP relay use Option 61 ruler to relay DHCP packet.
 disable - Disables the function DHCP relay use Option 61 ruler to relay DHCP packet.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the state of dhcp_relay Option 61:

```
DWS-3160-24PC:admin# config dhcp_relay option_61 state enable
Command: config dhcp_relay option_61 state enable

Success

DWS-3160-24PC:admin#
```

24-17 config dhcp_relay option_61 add

Description

This command is use to add a rule to determine the relay server based on Option 61. The match rule can base on either MAC address or a user-specified string. Only one relay server can be specified for a MAC-address or a string.

If relay servers are determined based on Option 60, and one relay server is determined based on Option 61, the final relay servers will be the union of these two sets of the servers.

Format

config dhcp_relay option_61 add [mac_address <macaddr> | string <desc_long 255>] [relay <ipaddr> | drop]

Parameters

mac_address - The client’s client-ID which is the hardware address of client.
 <macaddr> - Enter the client's MAC address here.

string - The client’s client-ID, which is specified by administrator.
 <desc_long 255> - Enter the client's description here. This value can be up to 255 characters long.

relay - Specifies to relay the packet to a IP address.
 <ipaddr> - Enter the IP address used for this configuration here.

drop - Specifies to drop the packet.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DHCP relay Option 61 function:

```
DWS-3160-24PC:admin# config dhcp_relay option_61 add mac_address 00-11-22-33-
44-55 drop
Command: config dhcp_relay option_61 add mac_address 00-11-22-33-44-55 drop

Success

DWS-3160-24PC:admin#
```

24-18 config dhcp_relay option_61 default

Description

This command is use to configure the default ruler for Option 61.

Format

config dhcp_relay option_61 default [relay <ipaddr> | drop]

Parameters

relay - Specifies to relay the packet that has no option matching 61 matching rules to an IP address.
<ipaddr> - Enter the IP address used for this configuration here.

drop - Specifies to drop the packet that have no Option 61 matching rules.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DHCP relay Option 61 function:

```
DWS-3160-24PC:admin# config dhcp_relay option_61 default drop
Command: config dhcp_relay option_61 default drop

Success

DWS-3160-24PC:admin#
```

24-19 config dhcp_relay option_61 delete

Description

This command is used to delete an Option 61 rule.

Format

config dhcp_relay option_61 delete [mac_address <macaddr> | string <desc_long 255> | all]

Parameters

mac_address - The entry with the specified MAC address will be deleted. **<macaddr>** - Enter the MAC address here.
string - The entry with the specified string will be deleted. **<desc_long 255>** - Enter the string value here. This value can be up to 255 characters long.
all - All rules excluding the default rule will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To remove a DHCP relay Option 61 entry:

```
DWS-3160-24PC:admin# config dhcp_relay option_61 delete mac_address 00-11-22-
33-44-55
Command: config dhcp_relay option_61 delete mac_address 00-11-22-33-44-55

Success

DWS-3160-24PC:admin#
```

24-20 show dhcp_relay option_61

Description

This command is used to display all rulers for Option 61.

Format

show dhcp_relay option_61

Parameters

None.

Restrictions

None.

Example

To display DHCP relay rulers for Option 61:

```
DWS-3160-24PC:admin# show dhcp_relay option_61
Command: show dhcp_relay option_61

Default Relay Rule: 10.90.90.200

Matching Rules:

Client-ID              Type         Relay Rule
---------------------- -----------  ----------------
abc                    String       Drop
abcde                  String       10.90.90.1
00-11-22-33-44-55      MAC Address  Drop

Total Entries: 3

DWS-3160-24PC:admin#
```

Chapter 25 DHCP Server Screening Command List

config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | ports [<portlist> | all] state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min | 30min] | trap_log [enable | disable]]
show filter dhcp_server

25-1 config filter dhcp_server

Description

This command is used to configure the state of the function for filtering of DHCP server packet and to add/delete the DHCP server/client binding entry. With DHCP server screening function, illegal DHCP server packet will be filtered.

This command is useful for projects that support per port control of the DHCP server screening function. The filter can be based on the DHCP server IP address, or based on a binding of the DHCP server IP and client MAC address.

The command has two purposes: To Specifies to filter all DHCP server packets on the specific port and to Specifies to allow some DHCP server packets with pre-defined server IP addresses and client MAC addresses. With this function, we can restrict the DHCP server to service specific DHCP clients. This is useful when two DHCP servers are present on the network, one of them provides the private IP address, and one of them provides the IP address.

Enabling filtering of the DHCP server port state will create one access profile and create one access rule per port (UDP port = 67). Filter commands in this file will share the same access profile.

Addition of a permit DHCP entry will create one access profile and create one access rule. Filtering commands in this file will share the same access profile.

Format

config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | ports [<portlist> | all] state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min | 30min] | trap_log [enable | disable]]

Parameters

add permit - Specifies to add a DHCP permit.
server_ip - The IP address of the DHCP server to be filtered. **<ipaddr>** - Enter the DHCP server IP address here.
client_mac - (Optional) The MAC address of the DHCP client. **<macaddr>** - Enter the DHCP client MAC address here.
ports - The port number of filter DHCP server. **<portlist>** - Enter the list of ports to be configured here. **all** - Specifies that all the port will be used for this configuration.
delete permit - Specifies to delete a DHCP permit.
server_ip - The IP address of the DHCP server to be filtered.

<ipaddr> - Enter the DHCP server IP address here.

client_mac - (Optional) The MAC address of the DHCP client.
<macaddr> - Enter the DHCP client MAC address here.

ports - The port number of filter DHCP server.
<portlist> - Enter the list of ports to be configured here.
all - Specifies that all the port will be used for this configuration.

state - Specifies to enable or disable the filter DHCP server state
enable - Specifies that the filter DHCP server state will be enabled.
disable - Specifies that the filter DHCP server state will be disabled.

illegal_server_log_suppress_duration - Specifies the same illegal DHCP server IP address detected will be logged only once within the duration. The default value is 5 minutes.
1min - Specifies that illegal server log suppress duration value will be set to 1 minute.
5min - Specifies that illegal server log suppress duration value will be set to 5 minutes.
30min - Specifies that illegal server log suppress duration value will be set to 30 minutes.

trap_log - Specifies if the trap/log option will be enabled or disabled.
enable - Specifies that the trap/log option will be enabled.
disable - Specifies that the trap/log option will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add an entry from the DHCP server/client filter list in the Switch’s database:

```
DWS-3160-24PC:admin# config filter dhcp_server add permit server_ip 10.1.1.1
client_mac 00-00-00-00-00-01 port 1-24
Command: config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-
00-00-00-00-01 port 1-24

Success.

DWS-3160-24PC:admin# config filter dhcp_server ports 1-10 state enable
Command: config filter dhcp_server ports 1-10 state enable

Success.

DWS-3160-24PC:admin#
```

25-2 show filter dhcp_server

Description

This command is used to display the DHCP server/client filter list created on the Switch.

Format

show filter dhcp_server

Parameters

None.

Restrictions

None.

Example

To display the DHCP server/client filter list created on the Switch:

```
DWS-3160-24PC:admin#show filter dhcp_server
Command: show filter dhcp_server

Enabled Ports: 1-10

Trap & Log State: Disabled

Illegal Server Log Suppress Duration:5 minutes
Filter DHCP Server/Client Table
Server IP Address Client MAC Address  Port
----------------- ------------------  --------------------
10.1.1.1          00-00-00-00-00-01   1-24

 Total Entries: 1

DWS-3160-24PC:admin#
```

Chapter 26 D-Link License Management System (DLMS) Command List

install dlms activation_code <string 25>
show dlms license

26-1 install dlms activation_code

Description

This command is used to install a DLMS activation code. The activation code is a set of codes which activates and unlocks extra functions on the Switch.

Format

install dlms activation_code <string 25>

Parameters

<string 25> - Enter the DLMS activation code here. This code can be up to 25 characters long.

Restrictions

Only Administrators can issue this command.

Example

To input a legal activation code:

```
DWS-3160-24PC:admin# install dlms activation_code ABCDEF1234567890ABCDFE000
Command: install dlms activation_code ABCDEF1234567890ABCDFE000

Success.

Please reboot the device to active the license.

DWS-3160-24PC:admin#
```

To input an illegal activation code:

```
DWS-3160-24PC:admin# install dlms activation_code QpOnM09876kJiHg54321EdCbA
Command: install dlms activation_code QpOnM09876kJiHg54321EdCbA

Illegal activation code.

DWS-3160-24PC:admin#
```

26-2 show dlms license

Description

This command is used to display the license information.

Format

show dlms license

Parameters

None.

Restrictions

None.

Example

To display license information:

```
DWS-3160-24PC:admin#show dlms license
Command: show dlms license

 License Model       Activation Code             Time Remaining
--------------------------------------------------------------------------
 DWS-3160-AP12-LIC   ABCDEF1234567890ABCDFE000   No Limited
 DWS-3160-AP24-LIC   ABCDEF1234567890ABCDFE001   No Limited
 --------------------------------------------------------------------------
                                                                  * expired

 Total Model Entries: 2 ; Key Entries: 2

DWS-3160-24PC:admin#
```

Chapter 27 Ethernet Ring Protection Switching (ERPS) Command List

enable erps
disable erps
create erps raps_vlan <vlanid>
delete erps raps_vlan <vlanid>
config erps raps_vlan <vlanid> [state [enable | disable] | ring_mel <value 0-7> | ring_port [west [<port> | virtual_channel] | east [<port> | virtual_channel]] | rpl_port [west | east | none] | rpl_owner [enable | disable] | protected_vlan [add | delete] vlanid <vidlist> | sub_ring raps_vlan <vlanid> tc_propagation state [enable | disable] | [add | delete] sub_ring raps_vlan <vlanid> | revertive [enable | disable] | timer {holdoff_time <millisecond 0-10000> | guard_time <millisecond 10-2000> | wtr_time <min 5-12>}]
config erps log [enable | disable]
config erps trap [enable | disable]
show erps {raps_vlan <vlanid> {sub_ring}}

27-1 enable erps

Description

This command is used to enable the global ERPS function on a Switch. When both the global state and the specified ring ERPS state are enabled, the specified ring will be activated.

The global ERPS function cannot be enabled, when any ERPS ring on the device is enabled and the integrity of any ring parameter is not available. For each ring with the ring state enabled when ERPS is enabled, the following integrity will be checked:

1. R-APS VLAN is created.
2. The Ring port is a tagged member port of the R-APS VLAN.
3. The RPL port is specified if the RPL owner is enabled.
4. The RPL port is not specified as virtual channel.

Format

enable erps

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable ERPS:

```
DWS-3160-24PC:admin# enable erps
Command: enable erps

Success.

DWS-3160-24PC:admin#
```

27-2 disable erps

Description

This command is used to disable the global ERPS function on a Switch.

Format

disable erps

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable ERPS:

```
DWS-3160-24PC:admin# disable erps
Command: disable erps

Success.

DWS-3160-24PC:admin#
```

27-3 create erps raps_vlan

Description

This command is used to create an R-APS VLAN on a Switch. Only one R-APS VLAN should be used to transfer R-APS messages.

NOTE: The R-APS VLAN can only be created after it was created using the ‘create vlan’ command. In other words, a normal VLAN will be assigned to represent a R-APS VLAN.

Format

create erps raps_vlan <vlanid>

Parameters

raps_vlan - Specifies the VLAN which will be the R-APS VLAN.
<vlanid> - Enter the VLAN ID used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an R-APS VLAN:

```
DWS-3160-24PC:admin#create erps raps_vlan 100
Command: create erps raps_vlan 100

Success.

DWS-3160-24PC:admin#
```

27-4 delete erps raps_vlan

Description

This command is used to delete an R-APS VLAN on a Switch. When an R-APS VLAN is deleted, all parameters related to this R-APS VLAN will also be deleted. This command can only be issued when the ring is not active.

Format

delete erps raps_vlan <vlanid>

Parameters

raps_vlan - Specifies the VLAN which will be the R-APS VLAN.
<vlanid> - Enter the VLAN ID used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an R-APS VLAN:

```
DWS-3160-24PC:admin# delete erps raps_vlan 100
Command: delete erps raps_vlan 100

Success.

DWS-3160-24PC:admin#
```

27-5 config erps raps_vlan

Description

This command is used to configure the ERPS R-APS VLAN settings.

The ring MEL is one field in the R-APS PDU.

NOTE: If CFM (Connectivity Fault Management) and ERPS are used at the same time, the R-APS PDU is one of a suite of Ethernet OAM PDU.

The behavior for forwarding of R-APS PDU should follow the Ethernet OAM. If the MEL of R-APS PDU is not higher than the level of the MEP with the same VLAN on the ring ports, the R-APS PDU cannot be forwarded on the ring.

Restrictions apply for ports that are included in a link aggregation group. A link aggregation group can be configured as a ring port by specifying the master port of the link aggregation port. Only the master port can be specified as a ring port. If the specified link aggregation group is eliminated, the master port retains its ring port status. If the ring port configured on virtual channel, the ring which the port connects to will be considered as a sub-ring.

NOTE: The ring ports cannot be modified when ERPS is enabled.

RPL port - Specifies one of the R-APS VLAN ring ports as the RPL port. To remove an RPL port from an R-APS VLAN, use the value ‘none’ in the designation for the RPL port.

RPL owner - Specifies the node as the RPL owner.

NOTE: The RPL port and RPL owner cannot be modified when ERPS is enabled; and the virtual channel cannot be configured as RPL. For example, if a ring port is configured on the virtual channel and the ring port is configured as an RPL port, an error message will be display and the configuration will fail.

The R-APS VLAN cannot be the protected VLAN. The protected VLAN can be one that has already been created, or it can be used for a VLAN that has not yet been created.

Holdoff timer - The Holdoff timer is used to filter out intermittent link faults when link failures occur during the protection switching process. When a ring node detects a link failure, it will start the holdoff timer and report the link failure event (R-APS BPDU with SF flag) after the link failure is confirmed within period of time specified.

Guard timer - Guard timer is used to prevent ring nodes from receiving outdated R-APS messages. This timer is used during the protection switching process after the link failure recovers. When the link node detects the recovery of the link, it will report the link failure recovery event (R-APS PDU with NR flag) and start the guard timer. Before the guard timer expires, all received R-APS messages are ignored by this ring node, except in the case where a burst of three R-APS event messages that indicates the topology of a sub-ring has changed and the node needs to flush FDB are received on the node. In this case the recovered link does not go into a blocking state. The Guard Timer should be greater than the maximum expected forwarding delay for which one R-APS message circles around the ring.

WTR timer - WTR timer is used to prevent frequent operation of the protection Switch due to an intermittent defect. This timer is used during the protection switching process when a link failure recovers. It is only used by the RPL owner. When the RPL owner in protection state receives R-APS PDU with an NR flag, it will start the WTR timer. The RPL owner will block the original unblocked RPL port and start to send R-APS PDU with an RB flag after the link recovery is confirmed within this period of time.

When both the global state and the specified ring ERPS state are enabled, the specified ring will be activated. STP and LBD should be disabled on the ring ports before the specified ring is activated.

The ring cannot be enabled before the R-APS VLAN is created, and ring ports, RPL port, RPL owner, are configured.

NOTE: These parameters cannot be changed when the ring is activated.

In order to guarantee correct operation, the following integrity will be checked when the ring is enabled and the global ERPS state is enabled.

- R-APS VLAN is created.
- The Ring port is the tagged member port of the R-APS VLAN.
- The RPL port is specified if RPL owner is enabled.

Format

config erps raps_vlan <vlanid> [state [enable | disable] | ring_mel <value 0-7> | ring_port [west [<port> | virtual_channel] | east [<port> | virtual_channel]] | rpl_port [west | east | none] | rpl_owner [enable | disable] | protected_vlan [add | delete] vlanid <vidlist> | sub_ring raps_vlan <vlanid> tc_propagation state [enable | disable] | [add | delete] sub_ring raps_vlan <vlanid> | revertive [enable | disable] | timer {holdoff_time <millisecond 0-10000> | guard_time <millisecond 10-2000> | wtr_time <min 5-12>}]

Parameters

raps_vlan - Specifies the R-APS VLAN used.
<vlanid> - Enter the VLAN ID used here.

state - Specifies to enable or disable the specified ring.
enable - Enable the state of the specified ring.
disable - Disable the state of the specified ring. The default value is disabled.

ring_mel - Specifies the ring MEL of the R-APS function. The default ring MEL is 1.
<value 0-7> - Enter the ring MEL value here. This value should be between 0 and 7.

ring_port - Specifies the ring port used.

west - Specifies the port as the west ring port.
<port> - Enter the port number here.
virtual_channel - Specifies the port as west port on virtual channel.

east - Specifies the port as the east ring port.
<port> - Enter the port number here.
virtual_channel - Specifies the port as east port on virtual channel.

rpl_port - Specifies the RPL port used.
west - Specifies the west ring port as the RPL port.
east - Specifies the east ring port as the RPL port.
none - No RPL port on this node. By default, the node has no RPL port.

rpl_owner - Specifies to enable or disable the RPL owner node.

enable - Specifies the device as an RPL owner node.
disable - This node is not an RPL owner. By default, the RPS owner is disabled.

protected_vlan - Specifies to add or delete the protected VLAN group.
add - Add VLANs to the protected VLAN group.
delete - Delete VLANs from the protected VLAN group.

vlanid - Specifies the VLAN ID to be removed or added.
<vidlist> - Enter the VLAN ID list here.

sub_ring - Specifies that the sub-ring is being configured.

raps_vlan - Specifies the R-APS VLAN.
<vlanid> - Enter the VLAN ID used here.

tc_propagation - Specifies that the topology propagation state will be configured.

state - Specifies the topology propagation state.
enable - Enable the propagation state of topology change for the sub-ring.
disable - Disable the propagation state of topology change for the sub-ring. The default value is disabled.

add - Connect the sub-ring to another ring.
delete - Disconnect the sub-ring from the connected ring.

sub_ring - Specifies that the sub-ring is being configured.

raps_vlan - Specifies the R-APS VLAN.
<vlanid> - Enter the VLAN ID used here.

revertive - Specifies the state of the R-APS revertive option.
enable - Specifies that the R-APS revertive option will be enabled.
disable - Specifies that the R-APS revertive option will be disabled.

timer - Specifies the R-APS timer used.
holdoff_time - (Optional) Specifies the holdoff time of the R-APS function. The default holdoff time is 0 milliseconds.
<millisecond 0-10000> - Enter the hold off time value here. This value must be in the range of 0 to 10000 milliseconds.
guard_time - (Optional) Specifies the guard time of the R-APS function. The default guard time is 500 milliseconds.
<millisecond 10-2000> - Enter the guard time value here. This value must be in the range of 0 to 2000 milliseconds.
wtr_time - (Optional) Specifies the WTR time of the R-APS function.
<min 5-12> - Enter the WTR time range value here. The range is from 5 to 12 minutes. The default WTR time is 5 minutes.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the MEL of the ERPS ring for a specific R-APS VLAN:

```
DWS-3160-24PC:admin#config erps raps_vlan 100 ring_mel 2
Command: config erps raps_vlan 100 ring_mel 2

Success.

DWS-3160-24PC:admin#
```

To configure the ports of the ERPS ring for a specific R-APS VLAN:

```
DWS-3160-24PC:admin#config erps raps_vlan 100 ring_port west 5
Command: config erps raps_vlan 100 ring_port west 5

Success.

DWS-3160-24PC:admin#
```

To configure the RPL port or the RPL owner for a specific R-APS VLAN:

```
DWS-3160-24PC:admin#config erps raps_vlan 100 rpl_port west
Command: config erps raps_vlan 100 rpl_port west

Success.

DWS-3160-24PC:admin#
```

To configure the protected VLAN for a specific R-APS VLAN:

```
DWS-3160-24PC:admin#config erps raps_vlan 100 protected_vlan add vlanid 10-20
Command: config erps raps_vlan 100 protected_vlan add vlanid 10-20

Success.

DWS-3160-24PC:admin#
```

To configure the ring state of the ERPS:

```
DWS-3160-24PC:admin#config erps raps_vlan 100 state enable
Command: config erps raps_vlan 100 state enable

Success.

DWS-3160-24PC:admin#
```

To configure a sub-ring connected to another ring:

```
DWS-3160-24PC:admin#config erps raps_vlan 3 add sub_ring raps_vlan 100
Command: config erps raps_vlan 3 add sub_ring raps_vlan 100

Success.

DWS-3160-24PC:admin#
```

To configure the state of topology change propagation:

```
DWS-3160-24PC:admin#config erps raps_vlan 3 sub_ring raps_vlan 100
tc_propagation state enable
Command: config erps raps_vlan 3 sub_ring raps_vlan 100 tc_propagation state
enable

Success.

DWS-3160-24PC:admin#
```

27-6 config erps log

Description

This command is used to configure the log state of ERPS events.

Format

config erps log [enable | disable]

Parameters

log - Specifies to enable or disable the ERPS log state.
enable - Enter enable to enable the log state.
disable - Enter disable to disable the log state. The default value is disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the ERPS log state:

```
DWS-3160-24PC:admin# config erps log enable
Command: config erps log enable

Success.

DWS-3160-24PC:admin#
```

27-7 config erps trap

Description

This command is used to configure trap state of ERPS events.

Format

config erps trap [enable | disable]

Parameters

trap - Specifies to enable or disable the ERPS trap state.
enable - Enter enable to enable the trap state.
disable - Enter disable to disable the trap state. The default value is disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the trap state of the ERPS:

```
DWS-3160-24PC:admin# config erps trap enable
Command: config erps trap enable

Success.

DWS-3160-24PC:admin#
```

27-8 show erps

Description

This command is used to display ERPS configuration and operation information.

The port state of the ring port may be as "Forwarding", "Blocking", "Signal Fail". "Forwarding" indicates that traffic is able to be forwarded. "Blocking" indicates that traffic is blocked by ERPS and a signal failure is not detected on the port. "Signal Fail" indicates that a signal failure is detected on the port and traffic is blocked by ERPS.

The RPL owner administrative state could be configured to "Enabled" or "Disabled". But the RPL owner operational state may be different from the RPL owner administrative state, for example, the RPL owner conflict occurs. "Active" is used to indicate that the RPL owner administrative state is enabled and the device is operated as the active RPL owner. "Inactive" is used to indicate that the RPL owner administrative state is enabled, but the device is operated as the inactive RPL owner.

Format

show erps {raps_vlan <vlanid> {sub_ring}}

Parameters

raps_vlan - (Optional) Specifies the R-APS VLAN.
<vlanid> - Enter the VLAN ID used here.

sub_ring - (Optional) Display the sub-ring configuration information.

Restrictions

None.

Example

To display ERPS information:

```
DWS-3160-24PC:admin#show erps
Command: show erps

 Global Status              : Enabled
 Log Status                 : Enabled
 Trap Status                : Enabled
 ------------------------------------
 R-APS VLAN                 : 3
 ERPS Status                : Enabled
 Admin West Port            : 11
 Operational West Port      : 11   (Signal Fail)
 Admin East Port            : 12
 Operational East Port      : 12   (Signal Fail)
 Admin RPL Port             : None
 Operational RPL Port       : None
 Admin Owner                : Disabled
 Operational Owner          : Disabled
 Protected VLANs            :
 Ring MEL                   : 1
 Holdoff Time               : 0 milliseconds
 Guard Time                 : 500 milliseconds
 WTR Time                   : 5 minutes
 Revertive mode             : Enabled
 Current Ring State         : Protection

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

To display ERPS information of R-APS VLAN 3:

```
DWS-3160-24PC:admin#show erps raps_vlan 3 sub_ring
Command: show erps raps_vlan 3 sub_ring

 R-APS VLAN: 3
 Sub-Ring R-APS VLAN     TC Propagation State
 -------------------     ---------------------
 100                     Enabled

DWS-3160-24PC:admin#
```

Chapter 28 Filter Command List

config filter netbios [<portlist> | all] state [enable | disable]
show filter netbios
config filter extensive_netbios [<portlist> | all] state [enable | disable]
show filter extensive_netbios

28-1 config filter netbios

Description

This command is used to configure the Switch to deny the NETBIOS packets on specific ports.

Format

config filter netbios [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Specifies the list of ports used. **all** – Specifies that all the ports will be used for the configuration.
state- Specifies the state of the filter to block the NETBIOS packet. **enable** - Specifies that the state will be enabled. **disable** - Specifies that the state will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure filter netbios state:

```
DWS-3160-24PC:admin# config filter netbios 1-10 state enable
Command: config filter netbios 1-10 state enable

Success.

DWS-3160-24PC:admin#
```

28-2 show filter netbios

Description

This command is used to display the NETBIOS filter state on the Switch.

Format

show filter netbios

Parameters

None.

Restrictions

None.

Example

To display the DHCP server/client filter list created on the Switch:

```
DWS-3160-24PC:admin#show filter netbios
Command: show filter netbios

 Enabled Ports: 1-10

DWS-3160-24PC:admin#
```

28-3 config filter extensive_netbios

Description

This command is used to configure the Switch to filter NETBIOS packets over 802.3 flame on the specific ports.

Format

config filter extensive_netbios [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter the list of ports used for this configuration here. **all** – Specifies that all the ports will be used this configuration.
state - Enable or disable the filter to block the NETBIOS packet over 802.3 frame. **enable** - Specifies that the filter state will be enabled. **disable** - Specifies that the filter state will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure a DHCP client/server filter entry.

```
DWS-3160-24PC:admin# config filter extensive_netbios 1-10 state enable
Command: config filter extensive_netbios 1-10 state enable

Success.

DWS-3160-24PC:admin#
```

28-4 show filter extensive_netbios

Description

This command is used to display the extensive netbios state on the Switch.

Format

show filter extensive_netbios

Parameters

None.

Restrictions

None.

Example

To display the extensive state created on the Switch:

```
DWS-3160-24PC:admin#show filter extensive_netbios
Command: show filter extensive_netbios

 Enabled Ports: 1-10

DWS-3160-24PC:admin#
```

Chapter 29 Filter Database (FDB) Command List

create fdb <vlan_name 32> <macaddr> [port <port> | drop]

create fdb vlanid <vidlist> <macaddr> [port <port> | drop]

create multicast_fdb <vlan_name 32> <macaddr>

config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>

config fdb aging_time <sec 10-1000000>

config multicast vlan_filtering_mode [vlanid <vidlist> | vlan <vlan_name 32> | all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]

delete fdb <vlan_name 32> <macaddr>

clear fdb [vlan <vlan_name 32> | port <port> | all]

show multicast_fdb {[vlan <vlan_name 32> | vlanid <vidlist>] | mac_address <macaddr>}

show fdb {[port <port> | vlan <vlan_name 32> | vlanid <vidlist> | mac_address <macaddr> | static | aging_time | security | tunnel]}

show multicast vlan_filtering_mode {[vlanid < vidlist> | vlan <vlan_name 32>]}

29-1 create fdb

Description

This command is used to create a static entry in the unicast MAC address forwarding table (database).

Format

create fdb <vlan_name 32> <macaddr> [port <port> | drop]

Parameters

<vlan_name 32> - Specifies a VLAN name associated with a MAC address. The maximum length of the VLAN name is 32 bytes.

<macaddr> - The MAC address to be added to the static forwarding table.

port - The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.

<port> - Enter the port number corresponding to the MAC destination address here.

drop - Specifies the action drop to be taken.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a unicast MAC forwarding entry:

```
DWS-3160-24PC:admin# create fdb default 00-00-00-00-01-02 port 5
Command: create fdb default 00-00-00-00-01-02 port 5

Success.

DWS-3160-24PC:admin#
```

To filter a unicast MAC:

```
DWS-3160-24PC:admin# create fdb default 00-00-00-00-01-03 drop
Command: create fdb default 00-00-00-00-01-03 drop

Success.

DWS-3160-24PC:admin#
```

29-2 create fdb vlanid

Description

This command is used to create a static entry in the unicast MAC address forwarding table (database).

Format

create fdb vlanid <vidlist> <macaddr> [port <port> | drop]

Parameters

<vidlist> - Specifies a VLAN ID associated with a MAC address.

<macaddr> - The MAC address to be added to the static forwarding table.

port - The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.
  <port> - Enter the port number corresponding to the MAC destination address here.

drop - Specifies the action drop to be taken.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a unicast MAC forwarding entry:

```
DWS-3160-24PC:admin#create fdb vlanid 1 00-00-00-00-01-04 port 5
Command: create fdb vlanid 1 00-00-00-00-01-04 port 5

Success.

DWS-3160-24PC:admin#
```

To filter a unicast MAC:

```
DWS-3160-24PC:admin#create fdb vlanid 1 00-00-00-00-01-05 drop
Command: create fdb vlanid 1 00-00-00-00-01-05 drop

Success.

DWS-3160-24PC:admin#
```

29-3 create multicast_fdb

Description

This command is used to create a static entry in the multicast MAC address forwarding table (database).

Format

create multicast_fdb <vlan_name 32> <macaddr>

Parameters

<vlan_name 32> - The name of the VLAN on which the MAC address resides. The maximum name length is 32.

<macaddr> - The multicasts MAC address to be added to the static forwarding table.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a multicast MAC forwarding entry to the default VLAN:

```
DWS-3160-24PC:admin#create multicast_fdb default 01-00-5E-00-00-00
Command: create multicast_fdb default 01-00-5E-00-00-00

Success.

DWS-3160-24PC:admin#
```

29-4 config multicast_fdb

Description

This command is used to configure the Switch’s multicast MAC address forwarding database.

Format

config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>

Parameters

<vlan_name 32> - The name of the VLAN on which the MAC address resides. The maximum name length is 32.

<macaddr> - The MAC address that will be added or deleted to the forwarding table.

add - Specifies to add ports to the multicast forwarding table.
delete - Specifies to remove ports from the multicast forwarding table.

<portlist> - Specifies a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a multicast MAC forwarding entry to the default VLAN on port 1 to 5:

```
DWS-3160-24PC:admin#config multicast_fdb default 01-00-5E-00-00-00 add 1-5
Command: config multicast_fdb default 01-00-5E-00-00-00 add 1-5

Success.

DWS-3160-24PC:admin#
```

29-5 config fdb aging_time

Description

This command is used to configure the MAC address table aging time.

Format

config fdb aging_time <sec 10-1000000>

Parameters

aging_time - Specifies the FDB age out time in seconds. 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 10 to 1000000 seconds with a default value of 300 seconds. 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.
<sec 10-1000000> - The FDB age out time must be between 10 to 1000000 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the MAC address table aging time to 600 seconds:

```
DWS-3160-24PC:admin#config fdb aging_time 600
Command: config fdb aging_time 600

Success.

DWS-3160-24PC:admin#
```

29-6 config multicast vlan_filtering_mode

Description

This command is used to configure the multicast packet filtering mode for VLANs. The registered group will be forwarded to the range of ports in the multicast forwarding database.

Format

config multicast vlan_filtering_mode [vlanid <vidlist> | vlan <vlan_name 32> | all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]

Parameters

vlanid - Specifies a list of VLANs to be configured.
<vidlist> - Enter the VLAN ID list here.
vlan - Specifies the name of the VLAN. The maximum name length is 32.
<vlan_name 32> - The VLAN name can be up to 32 characters long.
all - Specifies all configured VLANs.

forward_all_groups - Both the registered group and the unregistered group will be forwarded to all member ports of the specified VLAN where the multicast traffic comes in.
forward_unregistered_groups - The unregistered group will be forwarded to all member ports of the VLAN where the multicast traffic comes in.
filter_unregistered_groups - The unregistered group will be filtered.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the multicast packet filtering mode to filter all unregistered multicast groups for the VLAN 200 to 300:

```
DWS-3160-24PC:admin#config multicast vlan_filtering_mode vlanid 100
forward_all_groups
Command: config multicast vlan_filtering_mode vlanid 100 forward_all_groups

Success.

DWS-3160-24PC:admin#
```

29-7 delete fdb

Description

This command is used to delete a static entry from the forwarding database.

Format

delete fdb <vlan_name 32> <macaddr>

Parameters

<vlan_name 32> - The name of the VLAN on which the MAC address resides. The maximum name length is 32.

<macaddr> - The multicast MAC address to be deleted from the static forwarding table.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a static FDB entry:

```
DWS-3160-24PC:admin# delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DWS-3160-24PC:admin#
```

29-8 clear fdb

Description

This command is used to clear the Switch's forwarding database for dynamically learned MAC addresses.

Format

clear fdb [vlan <vlan_name 32> | port <port> | all]

Parameters

vlan - Clears the FDB entry by Specifiesing the VLAN name.
<vlan_name 32> - The name of the VLAN on which the MAC address resides. The maximum name length is 32.

port - Clears the FDB entry by Specifiesing the port number.
<port> - The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.

all - Clears all dynamic entries in the Switch's forwarding database.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear all FDB dynamic entries:

```
DWS-3160-24PC:admin# clear fdb all
Command: clear fdb all

Success.

DWS-3160-24PC:admin#
```

29-9 show multicast_fdb

Description

This command is used to display the multicast forwarding database of the Switch.

Format

show multicast_fdb {[vlan <vlan_name 32> | vlanid <vidlist>] | mac_address <macaddr>}

Parameters

vlan - (Optional) The name of the VLAN on which the MAC address resides.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - (Optional) Displays the entries for the VLANs indicated by VID list.
<vidlist> - Enter the VLAN ID list here.

mac_address - (Optional) Specifies a MAC address, for which FDB entries will be displayed.
<macaddr> - Enter the MAC address here.

If no parameter is specified, all multicast FDB entries will be displayed.

Restrictions

None.

Example

To display the multicast MAC address table:

```
DWS-3160-24PC:admin#show multicast_fdb
Command: show multicast_fdb

 VLAN Name      : default
 MAC Address    : 01-00-5E-00-00-00
 Egress Ports   : 1-5
 Mode           : Static

Total Entries: 1

DWS-3160-24PC:admin#
```

29-10 show fdb

Description

This command is used to display the current unicast MAC address forwarding database.

Format

show fdb {[port <port> | vlan <vlan_name 32> | vlanid <vidlist> | mac_address <macaddr> | static | aging_time | security | tunnel]}

Parameters

port - (Optional) Displays the entries for a specified port.
<port> - Enter the port number here.

vlan - (Optional) Displays the entries for a specific VLAN. The maximum name length is 32.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - (Optional) Displays the entries for the VLANs indicated by VID list.
<vidlist> - Enter the VLAN ID list here.

mac_address - (Optional) Displays a specific MAC address.
<macaddr> - Enter the MAC address here.

static - (Optional) Displays all permanent entries.

aging_time - (Optional) Displays the unicast MAC address aging time.

security - (Optional) Displays the FDB entries that are created by the security module.

tunnel - (Optional) Display all entries in the tunnel.

If no parameter is specified, system will display the unicast address table.

Restrictions

None.

Example

To display the FDB table:

```
DWS-3160-24PC:admin#show fdb
Command: show fdb

 Unicast MAC Address Aging Time  = 600

 VID  VLAN Name                        MAC Address       Port  Type    Status
 ---- -------------------------------- ----------------- ----- ------- -------
 1    default                          00-00-00-00-01-02 5     Static  Forward
 1    default                          00-00-00-00-01-03 -     Static  Drop
 1    default                          00-00-00-00-01-04 5     Static  Forward
 1    default                          00-00-00-00-01-05 -     Static  Drop
 1    default                          00-11-22-33-45-67 CPU   Self    Forward

Total Entries: 5

DWS-3160-24PC:admin#
```

To display the security FDB table:

```
DWS-3160-24PC:admin#show fdb security
Command: show fdb security

 VID  MAC Address       Port  Type    Status  Security Module
 ---- ----------------- ----- ------- ------- --------------------------------
 1    00-00-00-00-01-02 5     Static  Forward Compound Authentication
 1    00-00-00-00-01-04 5     Static  Forward Compound Authentication

Total Entries: 2

DWS-3160-24PC:admin#
```

29-11 show multicast vlan_filtering_mode

Description

This command is used to display the multicast packet filtering mode for VLANs.

NOTE: A product that supports the multicast VLAN filtering mode can not use the port filtering mode and the VLAN filtering mode at the same time.

Format

show multicast vlan_filtering_mode {[vlanid < vidlist> | vlan <vlan_name 32>]}

Parameters

vlanid - (Optional) Specifies a list of VLANs to be configured. **<vidlist>** - Enter the VLAN ID list here.
vlan - (Optional) Specifies the name of the VLAN. The maximum name length is 32. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
If no parameter is specified, the device will display all multicast filtering settings in the device.

Restrictions

None.

Example

To display the multicast vlan_filtering_mode for VLANs:

```
DWS-3160-24PC:admin#show multicast vlan_filtering_mode
Command: show multicast vlan_filtering_mode

VLAN ID/VLAN Name                           Multicast Filter Mode
----------------------------------------    -----------------------------
1   /default                                forward_unregistered_groups
2   /v2                                     forward_unregistered_groups
3   /v3                                     forward_unregistered_groups
100 /guestVLAN                              forward_all_groups

DWS-3160-24PC:admin#
```

Chapter 30 Flash File System (FFS) Command List

show storage_media_info

change drive <drive_id>

md <pathname 64>

rd <pathname 64>

cd {<pathname 64>}

dir {<pathname 64>}

rename <pathname 64> <filename 64>

del <pathname 64> {recursive}

erase <pathname 64>

move <pathname 64> <pathname 64>

copy <pathname 64> <pathname 64>

format <drive_id> {[fat16 | fat32]} {<label_name>}

30-1 show storage_media_info

Description

This command is used to display the information of the storage media available on the system. There can be one or multiple media on the system. The information for a media includes the drive number, the media identification.

Format

show storage_media_info

Parameters

None.

Restrictions

None.

Example

To display the storage media's information:

```
DWS-3160-24PC:admin#show storage_media_info
Command: show storage_media_info

Drive  Media Type      Size  Label        FS Type
-----  ----------  --------  -----------  -------
c:     Flash          28 MB               FFS

DWS-3160-24PC:admin#
```

30-2 change drive

Description

This command is used to change the current drive.

Format

change drive <drive_id>

Parameters

<drive_id> - Specifies the drive ID. The format of drive_id is C:/, D:/ etc.

Restrictions

None.

Example

To display the storage media's information:

```
DWS-3160-24PC:admin# change drive c:/
Command: change drive c:/

Success.

DWS-3160-24PC:admin#
```

30-3 md

Description

This command is used to create a directory.

Format

md <pathname 64>

Parameters

<pathname 64> - Specifies the directory to be removed. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory. The drive ID also included in this parameter, for example: d:/config/bootup.cfg. This name can be up to 64 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To make a directory:

```
DWS-3160-24PC:admin# md c:/abc
Command: md c:/abc

Success.

DWS-3160-24PC:admin#
```

30-4 rd

Description

This command is used to remove a directory. If there are files still existing in the directory, this command will fail and return error message.

Format

rd <pathname 64>

Parameters

<pathname 64> - Specifies the directory to be removed. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory. This name can be up to 64 characters long.	

Restrictions

Only Administrators and Operators can issue this command.

Example

To remove a directory:

```
DWS-3160-24PC:admin# rd c:/abc
Command: rd c:/abc

Success.

DWS-3160-24PC:admin#
```

30-5 cd

Description

This command is used to change the current directory. The current directory is changed under the current drive. If you want to change the working directory to the directory in another drive, then you need to change the current drive to the desired drive, and then change the current directory. The current drive and current directory will be displayed if the <pathname> is not specified.

Format

cd {<pathname 64>}

Parameters

<pathname 64> - (Optional) Specifies the directory to be removed. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory. This name can be up to 64 characters long.

Restrictions

None.

Example

To change to other directory or display current directory path:

```
DWS-3160-24PC:admin#cd
Command: cd

Current work directory: "/c:".

DWS-3160-24PC:admin#
```

30-6 dir

Description

This command is used to list all of the files located in a directory of a drive. If pathname is not specified, then all of the files in the specified drive will be displayed. If none of the parameters are specified, the files in the current drive will be displayed.

Format

dir {<pathname 64>}

Parameters

<pathname 64> - (Optional) Specifies the directory to be removed. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.

Restrictions

None.

Example

List the files:

```
DWS-3160-24PC:admin#dir
Command: dir

Directory of /c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1 CFG(*)  -rw- 80878    2000/01/28 23:17:20 config.cfg
  2         drw- 0        2000/01/01 00:09:17 wireless
  3 RUN(*)  -rw- 8235804  2000/01/21 03:32:05 runtime.had
  4         d--- 0        2000/01/28 21:53:55 system

29618 KB total (21363 KB free)
(*) -with boot up info          (b) -with backup info

DWS-3160-24PC:admin#
```

30-7 rename

Description

This command is used to rename a file. This command is used to rename a file in the file system. The pathname specifies the file (in path form) to be renamed and the filename specifies the new filename. If the pathname is not a full path, then it refers to a path under the current directory for the drive. The renamed file will stay in the same directory.

Format

rename <pathname 64> <filename 64>

Parameters

<pathname 64> - Specified the file (in path form) to be renamed. This name can be up to 64 characters long.

<filename 64> - Specified the new name of the file. This name can be up to 64 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To rename a file:

```
DWS-3160-24PC:admin# rename run.had run1.had
Command: rename run.had run1.had

Success.

DWS-3160-24PC:admin#
```

30-8 del

Description

This command is used to delete a file, either physically or softly. It is also used to delete a directory and its contents. If two files with the same name under the same directory are softly deleted sequentially, only the last one will exist. Deleting, copying, renaming or moving the already softly deleted file is not acceptable.

System will prompt if the target file is a FW or configuration whose type is boot up or backup.

Format

del <pathname 64> {recursive}

Parameters

<pathname 64> - Specifies the file or directory to be deleted. If it is specified in the associated form, then it is related to the current directory. This name can be up to 64 characters long.
recursive - (Optional) Used on directory, to delete a directory and its contents even if it's not empty.

Restrictions

Only Administrators and Operators can issue this command.

Example

Delete a directory with parameter "recursive":

```
DWS-3160-24PC:admin#dir
Command: dir

Directory of /c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1         drw- 0        2000/01/15 03:55:26 12
  2 CFG(*)  -rw- 77149    2000/01/15 03:26:52 config.cfg
  3         drw- 0        2000/01/01 00:09:17 wireless
  4 RUN(*)  -rw- 8236612  2000/01/01 00:03:36 runtime.had
  5         d--- 0        2000/01/15 03:22:33 system

29618 KB total (21368 KB free)
(*) -with boot up info          (b) -with backup info

DWS-3160-24PC:admin#del 12 recursive
Command: del 12 recursive

Success.

DWS-3160-24PC:admin#dir
Command: dir

Directory of /c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1 CFG(*)  -rw- 77149    2000/01/15 03:26:52 config.cfg
  2         drw- 0        2000/01/01 00:09:17 wireless
  3 RUN(*)  -rw- 8236612  2000/01/01 00:03:36 runtime.had
  4         d--- 0        2000/01/15 03:22:33 system

29618 KB total (21369 KB free)
(*) -with boot up info          (b) -with backup info

DWS-3160-24PC:admin#
```

30-9 erase

Description

This command is used to delete a file stored in the file system.

System will prompt if the target file is a FW or configuration whose type is boot up.

Format

erase <pathname 64>

Parameters

<pathname 64> - Specifies the file to be deleted. If it is specified in the associated form, then it is related to the current directory. This name can be up to 64 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To erase a file:

```
DWS-3160-24PC:admin#dir
Command: dir

Directory of /c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1 CFG(*)  -rw- 77149    2000/01/15 03:26:52 config.cfg
  2         drw- 0        2000/01/01 00:09:17 wireless
  3 RUN(*)  -rw- 8236612  2000/01/01 00:03:36 runtime.had
  4         d--- 0        2000/01/15 03:22:33 system
  1 CFG(*)  -rw- 77149    2000/01/15 03:28:52 config2.cfg

29618 KB total (21292 KB free)
(*) -with boot up info          (b) -with backup info

DWS-3160-24PC:admin#erase config2.cfg
Command: erase config2.cfg

Success.

DWS-3160-24PC:admin#dir
Command: dir

Directory of /c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1 CFG(*)  -rw- 77149    2000/01/15 03:26:52 config.cfg
  2         drw- 0        2000/01/01 00:09:17 wireless
  3 RUN(*)  -rw- 8236612  2000/01/01 00:03:36 runtime.had
  4         d--- 0        2000/01/15 03:22:33 system

29618 KB total (21369 KB free)
(*) -with boot up info          (b) -with backup info

DWS-3160-24PC:admin#
```

30-10 move

Description

This command is used to move a file around the file system.

NOTE: When a file is moved, it can be renames at the same time too.

Format

move <pathname 64> <pathname 64>

Parameters

<pathname 64> - Specifies the file to be moved. The path name can be specified either as a full path name or partial name. Specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory. This name can be up to 64 characters long.

<pathname 64> - Specifies the new path where the file will be moved. The path name can be. For partial path name, it indicates the file is in the current directory. This name can be up to 64 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To move a file from one location to another location:

```
DWS-3160-24PC:admin# move c:/log.txt c:/log1.txt
Command: move c:/log.txt c:/log1.txt

Success.

DWS-3160-24PC:admin#
```

30-11 copy

Description

This command is used to copy a file to another file in the file system.

Format

copy <pathname 64> <pathname 64>

Parameters

<pathname 64> - Specifies the file to be copied. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.

This name can be up to 64 characters long.

<pathname 64> - Specifies the file to copy to. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory. This name can be up to 64 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To copy a file:

```
DWS-3160-24PC:admin# copy c:/log.txt c:/log1.txt
Command: copy c:/log.txt c:/log1.txt

Success.

DWS-3160-24PC:admin#
```

30-12 format

Description

This command is used to format a specific drive.

Format

format <drive_id> {[fat16 | fat32]} {<label_name>}

Parameters

<drive_id> - Specifies drive to be formatted.

fat16 - Specifies a FAT16 file system

fat32 - Specifies a FAT32 file system

<label_name> - (Optional) Enter the label for the drive here. This value can be up to 8 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To format a drive:

```
DWS-3160-24PC:admin#format d: fat32 aaaa
Command: format d: fat32 aaaa

 Formatting........................... Done

Success

DWS-3160-24PC:admin#
```

Chapter 31 Gratuitous ARP Command List

config gratuitous_arp send ipif_status_up [enable | disable]
config gratuitous_arp send dup_ip_detected [enable | disable]
config gratuitous_arp learning [enable | disable]
config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>
enable gratuitous_arp {ipif <ipif_name 12>} {trap **|** log}(1)
disable gratuitous_arp {ipif <ipif_name 12>} {trap **|** log}(1)
show gratuitous_arp {ipif <ipif_name>}

31-1 config gratuitous_arp send ipif_status_up

Description

The command is used to enable or disable sending of gratuitous ARP request packet while IPIF interface become up. This is used to automatically announce the interface’s IP address to other nodes. By default, the state is disabled, and only one gratuitous ARP packet will be broadcast.

Format

config gratuitous_arp send ipif_status_up [enable | disable]

Parameters

enable - Enable sending of gratuitous ARP when IPIF status become up.
disable - Disable sending of gratuitous ARP when IPIF status become up.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable send gratuitous ARP request in normal situation:

```
DWS-3160-24PC:admin# config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.

DWS-3160-24PC:admin#
```

31-2 config gratuitous_arp send dup_ip_detected

Description

The command is used to enable or disable sending of gratuitous ARP request packet while duplicate IP is detected. By default, the state is disabled. For this command, the duplicate IP detected means that the system received a ARP request packet that is sent by an IP address that match the system's own IP address. In this case, the system knows that somebody out there uses an IP address that is conflict with the system. In order to reclaim the correct host of this IP address, the system can send out the gratuitous ARP request packet for this duplicate IP address.

Format

config gratuitous_arp send dup_ip_detected [enable | disable]

Parameters

enable - Enable sending of gratuitous ARP when duplicate IP is detected.
disable - Disable sending of gratuitous ARP when duplicate IP is detected.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable send gratuitous ARP request when duplicate IP is detected:

```
DWS-3160-24PC:admin# config gratuitous_arp send dup_ip_detected enable
Command: config gratuitous_arp send dup_ip_detected enable

Success.

DWS-3160-24PC:admin#
```

31-3 config gratuitous_arp learning

Description

This command is used to enable or disable learning of ARP entry in ARP cache based on the received gratuitous ARP packet. Normally, the system will only learn the ARP reply packet or a normal ARP request packet that asks for the MAC address that corresponds to the system's IP address. The gratuitous ARP packet is sent by a source IP address that is identical to the IP that the packet is queries for.

NOTE: With the gratuitous ARP learning, the system will not learn new entry but only do the update on the ARP table based on the received gratuitous ARP packet.

Format

config gratuitous_arp learning [enable | disable]

Parameters

enable - Enable learning of ARP entry based on the received gratuitous ARP packet.
disable - Disable learning of ARP entry based on the received gratuitous ARP packet. This is the default option.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To display the global Gratuitous ARP state:

```
DWS-3160-24PC:admin# config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable

Success.

DWS-3160-24PC:admin#
```

31-4 config gratuitous_arp send periodically

Description

The command is used to configure the interval for periodical sending of gratuitous ARP request packet. By default, the interval is 0.

Format

config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>

Parameters

ipif - Interface name of Layer 3 interface.

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.

interval - Periodically send gratuitous ARP interval time in seconds. 0 means not send gratuitous ARP periodically.

<value 0-65535> - Enter the gratuitous ARP interval time here. This value must be between 0 and 65535 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure gratuitous ARP interval to 5 for IPIF System:

```
DWS-3160-24PC:admin# config gratuitous_arp send periodically ipif System
interval 5
Command: config gratuitous_arp send periodically ipif System interval 5

Success.

DWS-3160-24PC:admin#
```

31-5 enable gratuitous_arp

Description

The command is used to enable gratuitous ARP trap and log state. The Switch can trap and log the IP conflict event to inform the administrator. By default, trap is disabled and event log is enabled.

Format

enable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)

Parameters

ipif - (Optional) Interface name of Layer 3 interface

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.

trap - (Optional) Specifies to enable the trap function.

log - (Optional) Specifies to enable the log function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the system interface’s gratuitous ARP log and trap:

```
DWS-3160-24PC:admin#enable gratuitous_arp ipif System trap log
Command: enable gratuitous_arp ipif System trap log

Success.

DWS-3160-24PC:admin#
```

31-6 disable gratuitous_arp

Description

The command is used to disable gratuitous ARP trap and log state. The Switch can trap and log the IP conflict event to inform the administrator. By default, trap is disabled and event log is enabled.

Format

disable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)

Parameters

ipif - (Optional) Interface name of Layer 3 interface

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.

trap - (Optional) Specifies to disable the trap function.

log - (Optional) Specifies to disable the log function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable system interface’s gratuitous ARP log and trap:

```
DWS-3160-24PC:admin# disable gratuitous_arp ipif System trap log
Command: disable gratuitous_arp ipif System trap log

Success.

DWS-3160-24PC:admin#
```

31-7 show gratuitous_arp

Description

This command is used to display the gratuitous ARP configuration.

Format

show gratuitous_arp {ipif <ipif_name>}

Parameters

ipif - (Optional) Interface name of Layer 3 interface.
  <ipif_name> - Enter the IP interface name here.

Restrictions

None.

Example

To display gratuitous ARP log and trap state:

```
DWS-3160-24PC:admin#show gratuitous_arp
Command: show gratuitous_arp

Send on IPIF Status Up        : Enabled
Send on Duplicate IP Detected : Enabled
Gratuitous ARP Learning       : Enabled

IP Interface Name : Inter2
        Gratuitous ARP Trap                     : Disabled
        Gratuitous ARP Log                      : Enabled
        Gratuitous ARP Periodical Send Interval : 0

IP Interface Name : System
        Gratuitous ARP Trap                     : Enabled
        Gratuitous ARP Log                      : Enabled
        Gratuitous ARP Periodical Send Interval : 5

Total Entries: 2

DWS-3160-24PC:admin#
```

Chapter 32 IGMP Snooping Command List

config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_leave [enable | disable] | report_suppression [enable | disable]}(1)

config igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]

config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-3>}(1)

config router_ports [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

config router_ports_forbidden [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

enable igmp_snooping

disable igmp_snooping

create igmp_snooping static_group [vlan<vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

delete igmp_snooping static_group [vlan<vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>

show igmp_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>}

config igmp_snooping data_driven_learning [all | vlan_name <vlan_name> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)

config igmp_snooping data_driven_learning max_learned_entry <value 1-1024>

clear igmp_snooping data_driven_group [all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipaddr> | all]]

show igmp_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

show igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]

show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipaddr>}} {data_driven}

show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

show router_ports {[vlan <vlan_name 32> | vlanid <vlanid_list>]} {static | dynamic | forbidden}

show igmp_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist>]

clear igmp_snooping statistics counter

32-1 config igmp_snooping

Description

This command is used to configure IGMP snooping on the Switch.

Format

config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_leave [enable | disable] | report_suppression [enable | disable]}(1)

Parameters

vlan_name - Specifies the name of the VLAN for which IGMP snooping is to be configured.

<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters

long.

vlanid - Specifies the VLAN ID for which IGMP snooping is to be configured.

<vlanid_list> - Enter the VLAN ID here.

all - Specifies to use all configured VLANs.

state - (Optional) Enable or disable IGMP snooping for the chosen VLAN.

enable - Enter enable to enable IGMP snooping for the chosen VLAN.

disable - Enter disable to disable IGMP snooping for the chosen VLAN.

fast_leave - Enable or disable the IGMP snooping fast leave function.

enable - Enter enable to enable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receives the IGMP leave message.

disable - Enter disable to disable the IGMP snooping fast leave function.

report_suppression - When IGMP report suppression is enabled (the default), the Switch sends the first IGMP report from all hosts for a group to all the multicast routers. The Switch does not send the remaining IGMP reports for the group to the multicast routers. If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the Switch forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the Switch forwards all IGMPv3 reports for a group to the multicast devices.

enable - Enter enable to enable the report suppression function.

disable - Enter disable to disable the report suppression function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure IGMP snooping:

```
DWS-3160-24PC:admin#config igmp_snooping vlanid 2 state enable
Command: config igmp_snooping vlanid 2 state enable

Success.

DWS-3160-24PC:admin#
```

32-2 config igmp_snooping rate_limit

Description

This command is used to configure the rate of IGMP control packet that is allowed per port or per VLAN.

Format

config igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]

Parameters

ports - Specifies a range of ports to be configured.

<portlist> - Enter the range of ports to be configured here.

vlanid - Specifies a range of VLANs to be configured.

<vlanid_list> - Enter the VLAN ID list here.

<value 1-1000> - Configure the rate of the IGMP control packet that the Switch can process on a specific port/VLAN. The rate is specified in packets per second. The packets that exceed the limit will be dropped.

no_limit - Configure the rate of the IGMP control packet to be unlimited that the Switch can process on a specific port/VLAN. The rate is specified in packets per second. The packets that exceed the limit will be dropped. The default setting is no_limit.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the IGMP snooping per port rate_limit:

```
DWS-3160-24PC:admin# config igmp_snooping rate_limit ports 1 100
Command: config igmp_snooping rate_limit ports 1 100

Success.

DWS-3160-24PC:admin#
```

32-3 config igmp_snooping querier

Description

This command is used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members, and the permitted packet loss that guarantees IGMP snooping.

Format

config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-3>}(1)

Parameters

vlan_name - Specifies the name of the VLAN for which IGMP snooping querier is to be configured.

<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - Specifies the VLAN ID for which IGMP snooping querier is to be configured.

<vlanid_list> - Enter the VLAN ID list here.

all - Specifies all VLANs for which IGMP snooping querier is to be configured.

query_interval - (Optional) Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.

<sec 1-65535> - Enter the query interval value here. This value must between 1 and 65535 seconds.

max_reponse_time - (Optional) Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.

<sec 1-25> - Enter the maximum response time value here. This value must be between 1 and 25 seconds.

robustness_variable - (Optional) Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals:

<value 1-7> - Enter the robustness variable value here. This value must be between 1 and 7. By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be loosely.

1. Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval).
2. Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval).
3. Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.

last_member_query_interval - (Optional) Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group. On receiving a leave message, the router will assume there are no local members on the interface if there are no reports received after the response time (which is last member query interval * robustness variable)

<sec 1-25> - Enter the last member query interval value here. This value must be between 1 and 25 seconds.

state - (Optional) If the state is enabled, it allows the Switch to be selected as an IGMP Querier (sends IGMP query packets). It the state is disabled, then the Switch cannot play the role as a querier. Note that if the Layer 3 router connected to the Switch provide only the IGMP proxy function but does not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not send the multicast-routing protocol packet, the port will be timed out as a router port.

enable - Enter enable to enable this state.

disable - Enter disable to disable this state.

version - (Optional) Specifies the version of IGMP packet that will be sent by this port. If an IGMP packet received by the interface has a version higher than the specified version, this packet will be dropped.

<value 1-3> - Enter the version number here. This value must be between 1 and 3.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the IGMP snooping querier:

```
DWS-3160-24PC:admin#config igmp_snooping querier vlanid 2 query_interval 125
state enable
Command: config igmp_snooping querier vlanid 2 query_interval 125 state enable

Success.

DWS-3160-24PC:admin#
```

32-4 config router_ports

Description

This command is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router, regardless of protocol.

Format

config router_ports [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Parameters

<vlan_name 32> - Specifies the name of the VLAN on which the router port resides.
vlanid - Specifies the ID of the VLAN on which the router port resides.
    <vlanid_list> - Enter the VLAN ID here.

add - Specifies to add the router ports.
delete - Specifies to delete the router ports.

<portlist> - Specifies a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set up static router ports:

```
DWS-3160-24PC:admin# config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

DWS-3160-24PC:admin#
```

32-5 config router_ports_forbidden

Description

This command is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.

Format

config router_ports_forbidden [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Parameters

<vlan_name 32> - Specifies the name of the VLAN on which the router port resides.
vlanid - Specifies the ID of the VLAN on which the router port resides.
    <vlanid_list> - Enter the VLAN ID list here.

add - Specifies to add the router ports. **delete** - Specifies to delete the router ports.
<portlist> - Specifies a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set up port range 1-10 to forbidden router ports of default VLAN:

```
DWS-3160-24PC:admin#config router_ports_forbidden default add 20
Command: config router_ports_forbidden default add 20

Success.

DWS-3160-24PC:admin#
```

32-6 enable igmp_snooping

Description

This command is used to enable IGMP snooping on the Switch.

Format

enable igmp_snooping

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable IGMP snooping on the Switch:

```
DWS-3160-24PC:admin# enable igmp_snooping
Command: enable igmp_snooping

Success.

DWS-3160-24PC:admin#
```

32-7 disable igmp_snooping

Description

This command is used to disable IGMP snooping on the Switch. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface.

NOTE: Disabling IGMP snooping will also disable the forward multicast router only function.

Format

disable igmp_snooping

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable IGMP snooping on the Switch:

```
DWS-3160-24PC:admin# disable igmp_snooping
Command: disable igmp_snooping

Success.

DWS-3160-24PC:admin#
```

32-8 create igmp_snooping static_group

Description

This command is used to create an IGMP snooping static group. Member ports can be added to the static group. The static member and the dynamic member port form the member ports of a group.

The static group will only take effect when IGMP snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the IGMP protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports.

For a Layer 3 device, the device is also responsible to route the packet destined for this specific group to static member ports.

The static member port will only affect the IGMPv2 operation.

The Reserved IP multicast address 224.0.0.X must be excluded from the configured group.

The VLAN must be created first before a static group can be created.

Format

create igmp_snooping static_group [vlan<vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

Parameters

vlan - Specifies the name of the VLAN on which the router port resides.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the router port resides.
<vlanid_list> - Enter the VLAN ID here.

<ipaddr> - Specifies the multicast group IP address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an IGMP snooping static group for VLAN 1, group 239.1.1.1:

```
DWS-3160-24PC:admin#create igmp_snooping static_group vlanid 2 239.1.1.1
Command: create igmp_snooping static_group vlanid 2 239.1.1.1

Success.

DWS-3160-24PC:admin#
```

32-9 delete igmp_snooping static_group

Description

This command is used to delete an IGMP snooping multicast static group. The deletion of an IGMP snooping static group will not affect the IGMP snooping dynamic member ports for a group.

Format

delete igmp_snooping static_group [vlan<vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

Parameters

vlan - Specifies the name of the VLAN on which the router port resides.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the router port resides.
<vlanid_list> - Enter the VLAN ID list here.

<ipaddr> - Specifies the multicast group IP address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an IGMP snooping static group for VLAN 1, group 239.1.1.1:

```
DWS-3160-24PC:admin#delete igmp_snooping static_group vlanid 2 239.1.1.1
Command: delete igmp_snooping static_group vlanid 2 239.1.1.1

Success.

DWS-3160-24PC:admin#
```

32-10 config igmp_snooping static_group

Description

This command is used to configure an IGMP snooping static group. When a port is configured as a static member port, the IGMP protocol will not operate on this port. For example, suppose that a port is a dynamic member port learned by IGMP. If this port is configured as a static member later, then the IGMP protocol will stop operating on this port. The IGMP protocol will resume once this port is removed from static member ports.

The static member port will only affect V2 IGMP operation.

Format

config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>

Parameters

vlan - Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long. **vlanid** - Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - Specifies the multicast group IP address (for Layer 3 Switch). **add** - Specifies to add the member ports. **delete** - Specifies to delete the member ports.
<portlist> - Specifies a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To unset port range 9-10 from IGMP snooping static member ports for group 239.1.1.1 on default VLAN:

```
DWS-3160-24PC:admin#config igmp_snooping static_group vlan v2 239.1.1.1 delete
24
Command: config igmp_snooping static_group vlan v2 239.1.1.1 delete 24

Success.

DWS-3160-24PC:admin#
```

32-11 show igmp_snooping static_group

Description

This command is used to display the IGMP snooping multicast group static members.

Format

show igmp_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>}

Parameters

vlan - Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long. **vlanid** - Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - Specifies the multicast group IP address.

Restrictions

None.

Example

To display all the IGMP snooping static groups:

```
DWS-3160-24PC:admin#show igmp_snooping static_group
Command: show igmp_snooping static_group

VLAN ID/Name                           IP Address       Static Member Ports
------------------------------------   ---------------  ----------------------
2   /v2                                239.1.1.1         20-23

 Total Entries : 1

DWS-3160-24PC:admin#
```

32-12 config igmp_snooping data_driven_learning

Description

This command is used to enable or disable the data driven learning of an IGMP snooping group.

When data-driven learning is enabled for the VLAN, when the Switch receives the IP multicast traffic on this VLAN, an IGMP snooping group will be created. That is, the learning of an entry is not activated by IGMP membership registration, but activated by the traffic. For an ordinary IGMP snooping entry, the IGMP protocol will take care of the aging out of the entry. For a data-driven entry, the entry can be specified not to be aged out or to be aged out by the aged timer.

When data driven learning is enabled, and the data driven table is not full, the multicast filtering mode for all ports is ignored. That is, the multicast packets will be forwarded to router ports. If the data driven learning table is full, the multicast packets will be forwarded according to the multicast filtering mode.

NOTE: If a data-driven group is created and IGMP member ports are learned later, the entry will become an ordinary IGMP snooping entry. That is, the aging out mechanism will follow the ordinary IGMP snooping entry.

Format

config igmp_snooping data_driven_learning [all | vlan_name <vlan_name> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)

Parameters

vlan_name - Specifies the VLAN name to be configured.
  <vlan_name> - Enter the VLAN name here.
vlanid - Specifies the VLAN ID to be configured.
  <vlanid_list> - Enter the VLAN ID here.
all - Specifies all VLANs to be configured.

state - (Optional) Specifies to enable or disable the data driven learning of an IGMP snooping group.
  enable - Enter enable to enable the data driven learning option. By default, the state is enabled.
  disable - Enter disable to disable the data driven learning option.

aged_out - (Optional) Enable or disable the aging out of the entry.
  enable - Enter enable to enable the aging out of the entry.
  disable - Enter disable to disable the aging out of the entry. By default, the state is disabled state.

expiry_time - (Optional) Specifies the data driven group lifetime in seconds. This parameter is valid only when aged_out is enabled.
  <sec 1-65535> - Enter the expiry time here. This value must be between 1 and 65535 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the data driven learning of an IGMP snooping group on the default VLAN:

```
DWS-3160-24PC:admin#config igmp_snooping data_driven_learning vlan v2 state
enable
Command: config igmp_snooping data_driven_learning vlan_name v2 state enable

Success.

DWS-3160-24PC:admin#
```

32-13 config igmp_snooping data_driven_learning max_learned_entry

Description

This command is used to configure the maximum number of groups that can be learned by data driven. When the table is full, the system will stop the learning of the new data-driven groups. Traffic for the new groups will be dropped.

Format

config igmp_snooping data_driven_learning max_learned_entry <value 1-1024>

Parameters

max_learned_entry - Specifies the maximum number of groups that can be learned by data driven. The suggested default setting is 56. This default setting may vary depending on projects.

<value 1-1024> - Enter the maximum learning entry value here. This value must be between 1 and 1024.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the maximum number of groups that can be learned by data driven:

```
DWS-3160-24PC:admin# config igmp_snooping data_driven_learning
max_learned_entry 50
Command: config igmp_snooping data_driven_learning max_learned_entry 50

Success.

DWS-3160-24PC:admin#
```

32-14 clear igmp_snooping data_driven_group

Description

This command is used to delete the IGMP snooping group(s) learned by data driven.

Format

clear igmp_snooping data_driven_group [all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipaddr> | all]]

Parameters

all - Specifies all VLANs to which IGMP snooping groups will be deleted.

vlan_name - Specifies the VLAN name.
  <vlan_name> - Enter the VLAN name here.
vlanid - Specifies the VLAN ID.
  <vlanid_list> - Enter the VLAN ID here.

<ipaddr> - Specifies the group’s IP address learned by data driven.
all - Delete all IGMP snooping groups of specified VLANs.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete all the groups learned by data-driven:

```
DWS-3160-24PC:admin# clear igmp_snooping data_driven_group all
Command: clear igmp_snooping data_driven_group all

Success.

DWS-3160-24PC:admin#
```

32-15 show igmp_snooping

Description

This command is used to display the current IGMP snooping configuration on the Switch.

Format

show igmp_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view the IGMP snooping configuration.
  <vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN for which you want to view the IGMP snooping configuration.
  <vlanid_list> - Enter the VLAN ID list here.

If the VLAN is not specified, the system will display all current IGMP snooping configurations.

Restrictions

None.

Example

To display IGMP snooping:

```
DWS-3160-24PC:admin#show igmp_snooping
Command: show igmp_snooping

 IGMP Snooping Global State              : Enabled
 Data Driven Learning Max Entries        : 50

 VLAN Name                     : default
 Query Interval                : 125
 Max Response Time             : 10
 Robustness Value              : 2
 Last Member Query Interval    : 1
 Querier State                 : Disabled
 Querier Role                  : Non-Querier
 Querier IP                    : 0.0.0.0
 Querier Expiry Time           : 0 secs
 State                         : Disabled
 Fast Leave                    : Disabled
 Rate Limit                    : No Limitation
 Report Suppression            : Enabled
 Version                       : 3
 Data Driven Learning State    : Enabled
 Data Driven Learning Aged Out : Disabled
 Data Driven Group Expiry Time : 260

 VLAN Name                     : v2
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

32-16 show igmp_snooping rate_limit

Description

This command is used to display the IGMP snooping rate limit setting.

Format

show igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]

Parameters

ports - Specifies the port range.
<portlist> - Enter the range of ports here.

vlanid - Specifies the VLAN range.
<vlanid_list> - Enter the VLAN ID list here.

Restrictions

None.

Example

To display the IGMP snooping rate limit for ports 1 to 5:

```
DWS-3160-24PC:admin#show igmp_snooping rate_limit ports 1-5
Command: show igmp_snooping rate_limit ports 1-5

 Port      Rate Limit
 --------  ---------------
 1         100
 2         No Limit
 3         No Limit
 4         No Limit
 5         No Limit

Total Entries: 5

DWS-3160-24PC:admin#
```

32-17 show igmp_snooping group

Description

This command is used to display the current IGMP snooping group configuration on the Switch.

Format

show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipaddr>}} {data_driven}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view IGMP snooping group information. If VLAN, ports and IP address are not specified, the system will display all current IGMP snooping group information.

<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - (Optional) Specifies the ID of the VLAN for which you want to view IGMP snooping group information.

<vlanid_list> - Enter the VLAN ID list here.

ports - (Optional) Specifies a list of ports for which you want to view IGMP snooping group information.

<portlist> - Enter the list of ports here.

<ipaddr> - (Optional) Specifies the group IP address for which you want to view IGMP snooping group information.

data_driven - (Optional) If data_driven is specified, only data driven groups will be displayed.

Restrictions

None.

Example

To display the IGMP snooping group:

```
DWS-3160-24PC:admin#show igmp_snooping group
Command: show igmp_snooping group


 Source/Group                  : NULL/239.1.1.1
 VLAN Name/VID                 : v2/2
 Member Ports                  : 23
 UP Time                       : 445
 Expiry Time                   : 87
 Filter Mode                   : EXCLUDE

 Total Entries: 1

DWS-3160-24PC:admin#
```

32-18 show igmp_snooping forwarding

Description

This command is used to display the Switch’s current IGMP snooping forwarding table. It provides an easy way for users to check the list of ports that the multicast group that comes from a specific sources will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding VLAN. The IGMP snooping further restricts the forwarding ports.

Format

show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view IGMP snooping forwarding table information.

<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - (Optional) Specifies the ID of the VLAN for which you want to view IGMP snooping forwarding table information.

<vlanid_list> - Enter the VLAN ID list here.

If no parameter is specified, the system will display all current IGMP snooping forwarding table entries of the Switch.

Restrictions

None.

Example

To display all IGMP snooping forwarding entries located on the Switch:

```
DWS-3160-24PC:admin#show igmp_snooping forwarding
Command: show igmp_snooping forwarding



 VLAN Name                     : v2
 Source IP                     : *
 Multicast Group               : 239.1.1.1
 Port Member                   : 23

 Total Entries : 1

DWS-3160-24PC:admin#
```

32-19 show router_ports

Description

This command is used to display the configured router ports on the Switch.

Format

show router_ports {[vlan <vlan_name 32> | vlanid <vlanid_list>]} {static | dynamic | forbidden}

Parameters

vlan - (Optional) Specifies the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long. **vlanid** - Specifies the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
static - (Optional) Displays router ports that have been statically configured.
dynamic - (Optional) Displays router ports that have been dynamically configured.
forbidden - (Optional) Displays forbidden router ports that have been statically configured.
If no parameter is specified, the system will display all currently configured router ports on the Switch.

Restrictions

None.

Example

To display router ports:

```
DWS-3160-24PC:admin#show router_ports all
Command: show router_ports all

VLAN Name                 : default
Static Router Port        : 1-10
Dynamic Router Port       :
Router IP                 :
Forbidden Router Port     : 20

VLAN Name                 : v2
Static Router Port        :
Dynamic Router Port       :
Router IP                 :
Forbidden Router Port     :

VLAN Name                 : v3
Static Router Port        :
Dynamic Router Port       :
Router IP                 :
Forbidden Router Port     :

VLAN Name                 : guestVLAN
Static Router Port        :
Dynamic Router Port       :
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

32-20 show igmp_snooping statistics counter

Description

This command is used to display the statistics counter for IGMP protocol packets that are received by the Switch since IGMP snooping was enabled.

Format

show igmp_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist>]

Parameters

vlan - Specifies a VLAN to be displayed.
    <vlan_name> - Enter the VLAN name here.

vlanid - Specifies a list of VLANs to be displayed.
    <vlanid_list> - Enter the VLAN ID list here.

ports - Specifies a list of ports to be displayed.
    <portlist> - Enter the list of port to be displayed here.

Restrictions

None.

Example

To display the IGMP snooping statistics counter:

```
DWS-3160-24PC:admin#show igmp_snooping statistic counter vlanid 2
Command: show igmp_snooping statistic counter vlanid 2



VLAN Name          : v2
--------------------------------------------------
Group Number       : 1

Receive Statistics
    Query
      IGMP v1 Query                     : 0
      IGMP v2 Query                     : 0
      IGMP v3 Query                     : 0
      Total                             : 0
      Dropped By Rate Limitation        : 0
      Dropped By Multicast VLAN         : 0

    Report & Leave
      IGMP v1 Report                    : 0
      IGMP v2 Report                    : 0
      IGMP v3 Report                    : 0
      IGMP v2 Leave                     : 0
      Total                             : 0
      Dropped By Rate Limitation        : 0
      Dropped By Max Group Limitation   : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

To display the IGMP snooping statistics counter for a port:

```
DWS-3160-24PC:admin#show igmp_snooping statistic counter ports 1
Command: show igmp_snooping statistic counter ports 1

Port #            : 1
--------------------------------------------------
Group Number      : 0

Receive Statistics
    Query
      IGMP v1 Query                    : 0
      IGMP v2 Query                    : 0
      IGMP v3 Query                    : 0
      Total                            : 0
      Dropped By Rate Limitation       : 0
      Dropped By Multicast VLAN        : 0

    Report & Leave
      IGMP v1 Report                   : 0
      IGMP v2 Report                   : 0
      IGMP v3 Report                   : 0
      IGMP v2 Leave                    : 0
      Total                            : 0
      Dropped By Rate Limitation       : 0
      Dropped By Max Group Limitation  : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

32-21 clear igmp_snooping statistics counter

Description

This command is used to clear the IGMP snooping statistics counter.

Format

clear igmp_snooping statistics counter

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear the IGMP snooping statistics counter:

```
DWS-3160-24PC:admin# clear igmp_snooping statistic counter
Command: clear igmp_snooping statistic counter

Success.

DWS-3160-24PC:admin#
```

Chapter 33 IGMP Snooping Multicast (ISM) VLAN Command List

create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}

config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ip <ipaddr> | remap_priority [<value 0-7> | none] {replace_priority}}(1)

create igmp_snooping multicast_vlan_group_profile <profile_name 1-32>

config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>

delete igmp_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]

show igmp_snooping multicast_vlan_group_profile {<profile_name 1-32>}

config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>

show igmp_snooping multicast_vlan_group {<vlan_name 32>}

delete igmp_snooping multicast_vlan <vlan_name 32>

enable igmp_snooping multicast_vlan

disable igmp_snooping multicast_vlan

config igmp_snooping multicast_vlan forward_unmatched [disable | enable]

show igmp_snooping multicast_vlan {<vlan_name 32>}

33-1 create igmp_snooping multicast_vlan

Description

This command is used to create an IGMP snooping multicast VLAN. More than one multicast VLANs can be created. Newly created IGMP snooping multicast VLANs must use a unique VLAN ID and name. They cannot use the VLAN ID or name of any existing 802.1Q VLAN.

Also keep in mind the following conditions:

- Multicast VLANs cannot be configured or displayed using 802.1Q VLAN commands.
- An IP interface cannot be bound to a multicast VLAN.
- The multicast VLAN snooping function co-exists with the 802.1Q VLAN snooping function.

Format

create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}

Parameters

<vlan_name 32> - Enter the multicast VLAN name here. This name can be up to 32 characters long.

<vlanid 2-4094> - Enter the multicast VLAN ID here. This value must be between 2 and 4094.

remap_priority - (Optional) Specifies the remap priority value, to be associated with the data traffic forwarded on the multicast VLAN.
<value 0-7> - Enter the remap priority value here. This value must be between 0 and 7.
none - Specifies that the remap priority value will be set to none. The packet's original priority

will be used. This is the default setting.

replace_priority - (Optional) Specifies that the packet's priority will be changed by the Switch, based on the remap priority. This flag will only take effect when the remap priority is set.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an IGMP snooping multicast VLAN with the VLAN name mv1 and the VID 2:

```
DWS-3160-24PC:admin#create igmp_snooping multicast_vlan mv1 2
Command: create igmp_snooping multicast_vlan mv1 2

Success.

DWS-3160-24PC:admin#
```

33-2 config igmp_snooping multicast_vlan

Description

This command is used to add member ports and source ports to a list of multicast VLAN member ports. Member ports automatically become untagged members of the multicast VLAN and source ports automatically become tagged members of the multicast VLAN. However, member ports of one multicast VLAN are allowed to overlap with member ports on a different multicast VLAN.

A multicast VLAN must first be created using the create igmp_snooping multicast_vlan command before the multicast VLAN can be configured.

Format

config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ip <ipaddr> | remap_priority [<value 0-7> | none] {replace_priority}}(1)

Parameters

multicast_vlan - The name of the multicast VLAN to be configured.
<vlan_name 32> - Enter the VLAN here. The VLAN name can be up to 32 characters long.

add - Specifies that the entry will be added to the specified multicast VLAN.
delete - Specifies that the entry will be deleted to the specified multicast VLAN.

member_port - (Optional) A member port or range of member ports to be added to the multicast VLAN. The specified range of ports will become untagged members of the multicast VLAN.
<portlist> - Enter the list of port to be configured here.

tag_member_port - (Optional) Specifies the port or range of ports that will become tagged members of the multicast VLAN.
<portlist> - Enter the list of port to be configured here.

source_port - (Optional) A port or range of ports to be added to the multicast VLAN.
<portlist> - Enter the list of port to be configured here.

untag_source_port - (Optional) Specifies the source port or range of source ports as untagged members of the multicast VLAN. The PVID of the untagged source port is automatically

changed to the multicast VLAN. Source ports must be either tagged or untagged for any single multicast VLAN, i.e. both types cannot be members of the same multicast VLAN.
<portlist> - Enter the list of port to be configured here.

state - (Optional) Used to Specifies if the multicast VLAN for a chosen VLAN should be enabled or disabled.
enable - Specifies to enable the multicast VLAN for a chosen VLAN.
disable - Specifies to disable the multicast VLAN for a chosen VLAN.

replace_source_ip - (Optional) Before forwarding the report packet sent by the host, the source IP address in the join packet must be replaced by this IP address. If none is specified, the source IP address will not be replaced.
<ipaddr> - Enter the replace source IP address here.

remap_priority - (Optional) The remap priority value to be associated with the data traffic to be forwarded on the multicast VLAN. If none is specified, the packet's original priority is used. The default setting is none.
<value 0-7> - Enter the remap priority value here. This value must be between 0 and 7.
none - Specifies that the remap priority value will be set to none.

replace_priority - (Optional) Specifies that the packet priority will be changed to the remap_priority, but only if remap_priority is set.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure an IGMP snooping multicast VLAN with the name "mv1", make ports 1 and 3 members of the VLAN, and set the state to enable:

```
DWS-3160-24PC:admin#config igmp_snooping multicast_vlan mv1 add member_port 1,3
state enable
Command: config igmp_snooping multicast_vlan mv1 add member_port 1,3 state
enable


Success.


DWS-3160-24PC:admin#
```

33-3 create igmp_snooping multicast_vlan_group_profile

Description

This command is used to create an IGMP snooping multicast group profile on the Switch.

Format

create igmp_snooping multicast_vlan_group_profile <profile_name 1-32>

Parameters

<profile_name 1-32> - Enter the multicast VLAN group profile name here. The name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an IGMP snooping multicast group profile with the name “IGroup”:

```
DWS-3160-24PC:admin#create igmp_snooping multicast_vlan_group_profile IGroup
Command: create igmp_snooping multicast_vlan_group_profile IGroup

Success.

DWS-3160-24PC:admin#
```

33-4 config igmp_snooping multicast_vlan_group_profile

Description

This command is used to configure an IGMP snooping multicast group profile on the Switch and add or delete multicast addresses for the profile.

Format

config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>

Parameters

multicast_vlan_group_profile - Specifies the multicast VLAN profile name. The maximum length is 32 characters.

<profile_name 1-32> - Enter the multicast VLAN group name here. This name can be up to 32 characters long.

add - Adds a multicast address list to or from this multicast VLAN profile. The <mcast_address_list> can be a continuous single multicast address, such as 225.1.1.1, 225.1.1.3, 225.1.1.8, a multicast address range, such as 225.1.1.1-225.2.2.2, or both of types, such as 225.1.1.1, 225.1.1.18-225.1.1.20

delete - Deletes a multicast address list to or from this multicast VLAN profile. The <mcast_address_list> can be a continuous single multicast addresses, such as 225.1.1.1, 225.1.1.3, 225.1.1.8, or a multicast address range, such as 225.1.1.1-225.2.2.2, or both types, such as 225.1.1.1, 225.1.1.18-225.1.1.20

<mcast_address_list> - Enter the multicast VLAN IP address here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add the single multicast address 225.1.1.1 and multicast range 225.1.1.10-225.1.1.20 to the IGMP snooping multicast VLAN profile named “IGroup”:

```
DWS-3160-24PC:admin#config igmp_snooping multicast_vlan_group_profile IGroup
add 225.1.1.1, 225.1.1.10-225.1.1.20
Command: config igmp_snooping multicast_vlan_group_profile IGroup add
225.1.1.1, 225.1.1.10-225.1.1.20

Success.

DWS-3160-24PC:admin#
```

33-5 delete igmp_snooping multicast_vlan_group_profile

Description

This command is used to delete an IGMP snooping multicast group profile from the Switch.

Format

delete igmp_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]

Parameters

profile_name - Specifies the multicast VLAN profile name.

<profile_name 1-32> - Enter the multicast VLAN profile name here. This name can be up to 32 characters long.

all - Specifies to delete all the multicast VLAN profiles.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an IGMP snooping multicast group profile with the name “FGroup”:

```
DWS-3160-24PC:admin#delete igmp_snooping multicast_vlan_group_profile
profile_name FGroup
Command: delete igmp_snooping multicast_vlan_group_profile profile_name FGroup

Success.

DWS-3160-24PC:admin#
```

33-6 show igmp_snooping multicast_vlan_group_profile

Description

This command is used to display IGMP snooping multicast VLAN group profiles.

Format

show igmp_snooping multicast_vlan_group_profile {<profile_name 1-32>}

Parameters

<profile_name 1-32> - (Optional) Enter the multicast VLAN group profile name here. The name can be up to 32 characters long.

If no parameter is specified, then all IGMP snooping multicast VLAN group profiles will be displayed.

Restrictions

None.

Example

To display all IGMP snooping multicast VLAN group profiles:

```
DWS-3160-24PC:admin#show igmp_snooping multicast_vlan_group_profile
Command: show igmp_snooping multicast_vlan_group_profile

Profile Name                     Multicast Addresses
-------------------------------- -------------------------------
IGroup                           225.1.1.1
                                 225.1.1.10-225.1.1.20

 Total Entries: 1

DWS-3160-24PC:admin#
```

33-7 config igmp_snooping multicast_vlan_group

Description

This command is used to configure the IGMP snooping profile learned with the specific multicast VLAN group.

The following two cases can be considered for examples:

- The multicast group is not configured, multicast VLANs do not have any member ports overlapping and the join packet received by the member port is learned on only the multicast VLAN that this port is a member of.
- The join packet is learned with the multicast VLAN that contains the destination multicast group. If the destination multicast group of the join packet cannot be classified into any multicast VLAN to which this port belongs, then the join packet will be learned on the natural VLAN of the packet.

NOTE: A profile cannot overlap in different multicast VLANs. Multiple profiles can be added to a multicast VLAN.

Format

config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>

Parameters

<vlan_name 32> - Enter the multicast VLAN name here. The VLAN name can be up to 32 characters long.

add – Specifies to associate an IGMP snooping profile to a multicast VLAN.
delete – Specifies to de-associate an IGMP snooping profile from a multicast VLAN.

profile_name - Specifies the IGMP snooping profile name.
<profile_name 1-32> - Enter the IGMP snooping profile name here. The name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add an IGMP snooping profile to a multicast VLAN group with the name “mv1”:

```
DWS-3160-24PC:admin#config igmp_snooping multicast_vlan_group mv1 add
profile_name IGroup
Command: config igmp_snooping multicast_vlan_group mv1 add profile_name IGroup

Success.

DWS-3160-24PC:admin#
```

33-8 show igmp_snooping multicast_vlan_group

Description

This command is used to display an IGMP snooping multicast VLAN group.

Format

show igmp_snooping multicast_vlan_group {<vlan_name 32>}

Parameters

<vlan_name 32> - (Optional) Enter the multicast VLAN name here. This can be up to 32 characters long.

If no parameter is specified, then all the IGMP snooping multicast VLAN groups will be displayed.

Restrictions

None.

Example

To display all IGMP snooping multicast VLAN groups configured on the Switch:

```
DWS-3160-24PC:admin#show igmp_snooping multicast_vlan_group
Command: show igmp_snooping multicast_vlan_group

VLAN Name                        VLAN ID        Multicast Group Profiles
-------------------------------  -------  ---------------------------------
mv1                              20        IGroup

DWS-3160-24PC:admin#
```

33-9 delete igmp_snooping multicast_vlan

Description

This command is used to delete an IGMP snooping multicast VLAN.

Format

delete igmp_snooping multicast_vlan <vlan_name 32>

Parameters

<vlan_name 32> -Enter the multicast VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an IGMP snooping multicast VLAN called “v10”:

```
DWS-3160-24PC:admin#delete igmp_snooping multicast_vlan v10
Command: delete igmp_snooping multicast_vlan v10

Success.

DWS-3160-24PC:admin#
```

33-10 enable igmp_snooping multicast_vlan

Description

This command is used to enable the IGMP snooping multicast VLAN function. By default, this features is disabled.

Format

enable igmp_snooping multicast_vlan

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the IGMP snooping multicast VLAN function globally:

```
DWS-3160-24PC:admin#enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan

Success.

DWS-3160-24PC:admin#
```

33-11 disable igmp_snooping multicast_vlan

Description

This command is used to disable the IGMP snooping multicast VLAN function. By default, this features is disabled.

Format

disable igmp_snooping multicast_vlan

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the IGMP snooping multicast VLAN function:

```
DWS-3160-24PC:admin#disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan

Success.

DWS-3160-24PC:admin#
```

33-12 config igmp_snooping multicast_vlan forward_unmatched

Description

This command is used to configure the forwarding mode for IGMP multicast VLAN unmatched packets. When the Switch receives an IGMP snooping packet, it will match the packet against the multicast profile to determine which multicast VLAN to associate with it. If the packet does not match all the profiles, the packet will be forwarded or dropped based on this configuration.

Format

config igmp_snooping multicast_vlan forward_unmatched [disable | enable]

Parameters

enable – Specifies that the packet will be flooded on the VLAN.

disable – Specifies that the packet will be dropped. This is the default option.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the forwarding mode for IGMP multicast VLAN unmatched packets:

```
DWS-3160-24PC:admin# config igmp_snooping multicast_vlan forward_unmatched
enable
Command: config igmp_snooping multicast_vlan forward_unmatched enable

Success.

DWS-3160-24PC:admin#
```

33-13 show igmp_snooping multicast_vlan

Description

This command is used to display information for an IGMP snooping multicast VLAN.

Format

show igmp_snooping multicast_vlan {<vlan_name 32>}

Parameters

<vlan_name 32> - (Optional) Enter the multicast VLAN name here. The VLAN name can be up to 32 characters long.

If no parameter is specified, then all IGMP snooping multicast VLAN entries will be displayed.

Restrictions

None.

Example

To display all IGMP snooping multicast VLAN entries:

```
DWS-3160-24PC:admin#show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

IGMP Multicast VLAN Global State        : Enabled
IGMP Multicast VLAN Forward Unmatched   : Disabled

VLAN Name                     :mv1
VID                           :2

Member(Untagged) Ports        :10
Tagged Member Ports           :
Source Ports                  :1
Untagged Source Ports         :
Status                        :Enabled
Replace Source IP             : 10.90.90.254
Remap Priority                :0 (Replaced)

 Total Entries: 1

DWS-3160-24PC:admin#
```

Chapter 34 IP-MAC-Port Binding (IMPB) Command List

config address_binding ip_mac ports [<portlist> | all] {arp_inspection [strict | loose | disable] | ip_inspection [enable | disable] | protocol [ipv4] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500>}

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}

delete address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]

delete address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>]

config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}

show address_binding {ports {<portlist>}}

show address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]

show address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>]

enable address_binding dhcp_snoop

disable address_binding dhcp_snoop

clear address_binding dhcp_snoop binding_entry ports [<portlist> | all]

show address_binding dhcp_snoop {max_entry {ports <portlist>}}

show address_binding dhcp_snoop binding_entry {port <port>}

config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-50> | no_limit]

enable address_binding trap_log

disable address_binding trap_log

config address_binding recover_learning ports [<portlist> | all]

34-1 config address_binding ip_mac

Description

This command is used to configure the state of IMPB on the Switch for each port.

Format

config address_binding ip_mac ports [<portlist> | all] {arp_inspection [strict | loose | disable] | ip_inspection [enable | disable] | protocol [ipv4] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500>}

Parameters

ports - Specifies the ports used for this configuration.
- **<portlist>** - Enter the list of ports used for this configuration here.
- **all** - Specifies that all the ports will be used.

arp_inspection - (Optional) Specifies that the ARP inspection option will be configured.
- **strict** - In this mode, all packets are dropped by default until a legal ARP or IP packets are detected.
- **loose** - In this mode, all packets are forwarded by default until an illegal ARP or broadcast IP packets are detected. If not specified strict or loose, default is strict.
- **disable** - Disable ARP inspection function. The default value is disabled.

ip_inspection - (Optional) Specifies that the IP inspection option will be configured.
- **enable** - Enable IP inspection function. The legal IP packets will be forward, while the illegal IP packets will be dropped.

disable - Disable IP inspection function. The default value is disabled.

protocol - (Optional) Specifies the version used.
ipv4 - Only IPv4 packets will be checked.

allow_zeroip - (Optional) Specifies whether to allow ARP packets with a source IP address of 0.0.0.0. If the IP address 0.0.0.0 is not configured in the binding list and this setting is enabled, ARP packets with the source IP address of 0.0.0.0 will be allowed; If the IP address 0.0.0.0 is not configured in the binding list and this setting is disabled, ARP packets with the source IP address of 0.0.0.0 will not be allowed. This option does not affect the IMPB ACL Mode.
enable - Specifies that the allow zero IP option will be enabled.
disable - Specifies that the allow zero IP option will be disabled.

forward_dhcppkt - (Optional) By default, DHCP packets with a broadcast DA will be flooded. When set to disabled, the broadcast DHCP packet received by the specified port will not be forwarded. This setting is effective when DHCP Snooping is enabled, in this case DHCP packets trapped by the CPU must be forwarded by the software. This setting controls the forwarding behavior in this situation.
enable - Specifies that the forward DHCP packets option will be enabled.
disable - Specifies that the forward DHCP packets option will be disabled.

stop_learning_threshold - (Optional) When the number of blocked entries exceeds the threshold, the port will stop learning new addresses. Packets with a new address will be dropped.
<int 0-500> - Enter the stop learning threshold value here. This value must be between 0 and 500.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable IMPB on port 1:

```
DWS-3160-24PC:admin# config address_binding ip_mac ports 1 arp_inspection
strict
Command: config address_binding ip_mac ports 1 arp_inspection strict

Success.

DWS-3160-24PC:admin#
```

34-2 create address_binding ip_mac

Description

This command is used to create an IMPB entry.

Format

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}

Parameters

ipaddress - Specifies the IP address used for the IMPB entry.
<ipaddr> - Enter the IP address used here.

mac_address - Specifies the MAC address used for the IMPB entry.

<macaddr> - Enter the MAC address used here.

ports - (Optional) Specifies the portlist the entry will apply to. If not ports are specified, the settings will be applied to all ports.
<portlist> - Enter a list of ports used for this configuration here.
all - Specifies that all the ports will be included.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an IMPB entry:

```
DWS-3160-24PC:admin#create address_binding ip_mac ipaddress 10.1.1.1
mac_address 00-00-00-00-00-11
Command: create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11


Success.


DWS-3160-24PC:admin#
```

34-3 delete address_binding blocked

Description

This command is used to delete a blocked entry from the address binding database.

Format

delete address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]

Parameters

blocked - Specifies the address database that the system has automatically learned and blocked.
all - Specifies that all the entries will be used.
vlan_name - Specifies the name of the VLAN to which the blocked MAC address belongs.
<vlan_name> - Enter the VLAN name here.
mac_address - Specifies the MAC address of the entry or the blocked MAC address.
<macaddr> - Enter the MAC address used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a blocked address:

```
DWS-3160-24PC:admin# delete address_binding blocked vlan_name v31 mac_address
00-00-00-00-00-11
Command: delete address_binding blocked vlan_name v31 mac_address 00-00-00-00-
00-11

Success.

DWS-3160-24PC:admin#
```

34-4 delete address_binding ip_mac

Description

This command is used to delete an IMPB entry from the address binding database.

Format

delete address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>]

Parameters

- **ip_mac** - Specifies the user created IMPB database.
  - **ipaddress** - Specifies the learned IP address of the entry in the database.
    - **<ipaddr>** - Enter the IP address used here.
  - **mac_address** - Specifies the MAC address used for this configuration.
    - **<macaddr>** - Enter the MAC address used here.
  - **all** - Specifies that all the MAC address will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an IMPB entry:

```
DWS-3160-24PC:admin# delete address_binding ip_mac ipaddress 10.1.1.1
mac_address 00-00-00-00-00-11
Command: delete address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11

Success.

DWS-3160-24PC:admin#
```

34-5 config address_binding ip_mac

Description

This command is used to update an IMPB entry.

Format

config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}

Parameters

ipaddress - Specifies the IP address of the entry being updated.
<ipaddr> - Enter the IP address used here.

mac_address - Specifies the MAC address of the entry being updated
<macaddr> - Enter the MAC address used here.

ports - (Optional) Specifies which ports are used for the IMPB entry being updated. If not specified, then it is applied to all ports.
<portlist> - Enter the list of port used here.
all - Specifies that all the ports will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure an IMPB entry:

```
DWS-3160-24PC:admin# config address_binding ip_mac ipaddress 10.1.1.1
mac_address 00-00-00-00-00-11
Command: config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11


Success.

DWS-3160-24PC:admin#
```

34-6 show address_binding

Description

This command is used to display the global IMPB configuration and ports.

Format

show address_binding {ports {<portlist>}}

Parameters

ports – (Optional) Specifies the ports for which the information is displayed. If not specified, all ports are displayed.
<portlist> - Enter the list of ports used here.

If no parameter is specified, then the global address binding configurations will be displayed.

Restrictions

None.

Example

To display the IMPB global configuration:

```
DWS-3160-24PC:admin#show address_binding
Command: show address_binding

Trap/Log          : Disabled
DHCP Snoop        : Disabled

DWS-3160-24PC:admin#
```

To display the IMPB ports:

```
DWS-3160-24PC:admin#show address_binding ports
Command: show address_binding ports


 ARP: ARP Inspection   IP: IP Inspection

 Port   ARP      IP     Protocol Zero IP   DHCP Packet  Stop Learning
                                                        Threshold/Mode
 ----- -------- --------  ----- ---------  -----------  --------------
 1     Strict   Disabled  IPv4  Not Allow  Forward      500/Normal
 2     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 3     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 4     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 5     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 6     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 7     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 8     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 9     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 10    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 11    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 12    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 13    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 14    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 15    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 16    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

34-7 show address_binding blocked

Description

This command is used to display the blocked MAC entries in the address binding database.

Format

show address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]

Parameters

blocked - Specifies the addresses in the database that the system has auto learned and blocked.
  all - Specifies that all the MAC addresses will be used.
  vlan_name - Specifies the name of the VLAN to which the blocked MAC address belongs.
    <vlan_name> - Enter the VLAN name used here.
  mac_address - Specifies the MAC address of the entry or the blocked MAC address.
    <macaddr> - Enter the MAC address of the entry or the blocked MAC address.

Restrictions

None.

Example

To display the IMPB entries that are blocked:

```
DWS-3160-24PC:admin#show address_binding blocked all
Command: show address_binding blocked all

 VID  VLAN Name                        MAC Address       Port
 ---- -------------------------------- ----------------- ----
 1     default                         00-01-02-03-29-38     7
 1     default                         00-0C-6E-5C-67-F4     7
 1     default                         00-0C-F8-20-90-01     7
 1     default                         00-0E-35-C7-FA-3F     7
 1     default                         00-0E-A6-8F-72-EA     7
 1     default                         00-0E-A6-C3-34-BE     7
 1     default                         00-11-2F-6D-F3-AC     7
 1     default                         00-50-8D-36-89-48     7
 1     default                         00-50-BA-00-05-9E     7
 1     default                         00-50-BA-10-D8-F6     7
 1     default                         00-50-BA-38-7D-E0     7
 1     default                         00-50-BA-51-31-62     7
 1     default                         00-50-BA-DA-01-58     7
 1     default                         00-A0-C9-01-01-23     7
 1     default                         00-E0-18-D4-63-1C     7

Total entries : 15

DWS-3160-24PC:admin#
```

34-8 show address_binding ip_mac

Description

This command is used to display the IMPB entries in the address binding database.

Format

show address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>]

Parameters

ip_mac -Specifies the user created IMPB database.
- **all** - Specifies that all the IP addresses will be used.
- **ipaddress** - Specifies the learned IP address of the entry in the database.
  - **<ipaddr>** - Enter the learned IP address here.
- **mac_address** - Specifies the MAC address of the entry in the database.
  - **<macaddr>** - Enter the MAC address here.

Restrictions

None.

Example

To display IMPB entries:

```
DWS-3160-24PC:admin#show address_binding ip_mac all
Command: show address_binding ip_mac all

 M(Mode) - D:DHCP, S:Static ACL - A:Active I:Inactive

 IP Address                              MAC Address       M  ACL Ports
 --------------------------------------- ----------------- -- -- --------------
-
 10.1.1.1                                00-00-00-00-00-11 S  I  1-24

Total Entries : 1

DWS-3160-24PC:admin#
```

34-9 enable address_binding dhcp_snoop

Description

This command is used to enable DHCP snooping mode. By default, DHCP snooping is disabled.

If a user enables DHCP Snooping mode, all ports which have IMPB disabled will become server ports. The Switch will learn the IP addresses through server ports (by using DHCP Offer and DHCP ACK packets).

NOTE: The DHCP discover packet cannot be passed through the user ports if the allow zero IP function is disabled on the port.

The auto-learned IMPB entry will be mapped to a specific source port based on the MAC address learning function. This entry will be created as an IP-Inspection mode binding entry for this specific port. Each entry is associated with a lease time. When the lease time has expires, the expired entry will be removed from the port. The auto-learned binding entry can be moved from one port to another port if the DHCP snooping function has learned that the MAC address has moved to a different port.

If a situation occurs where a binding entry learned by DHCP snooping conflicts with a statically configured entry. The binding relation has conflicted. For example, if IP A is binded to MAC X with a static configuration and suppose that the binding entry learned by DHCP snooping is that IP A is bound to MAC Y, and then it is conflict. When the DHCP snooping learned entry binds with the static configured entry, and the DHCP snooping learned entry will not be created.

In a situation where the same IMPB pair has been statically configured, the auto-learned entry will not be created. In a situation where the learned information is consistent with the statically configured entry the auto-learned entry will not be created. In a situation where the entry is statically configured in ARP mode the auto learned entry will not be created. In a situation where the entry is statically configured on one port and the entry is auto-learned on another port, the auto-learned entry will not be created.

Format

enable address_binding dhcp_snoop

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable DHCP IPv4 snooping mode:

```
DWS-3160-24PC:admin# enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DWS-3160-24PC:admin#
```

34-10 disable address_binding dhcp_snoop

Description

This command is used to disable DHCP snooping mode. When the DHCP snooping function is disabled, all of the auto-learned binding entries will be removed.

Format

disable address_binding dhcp_snoop

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable DHCP IPv4 snooping mode:

```
DWS-3160-24PC:admin# disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DWS-3160-24PC:admin#
```

34-11 clear address_binding dhcp_snoop binding_entry ports

Description

This command is used to clear the DHCP snooping entries learned for the specified ports.

Format

clear address_binding dhcp_snoop binding_entry ports [<portlist> | all]

Parameters

ports - Specifies the list of ports to clear the DHCP snooping learned entries.
<portlist> - Enter the list of ports used here
all - Specifies that all the ports will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear DHCP IPv4 snooping entries on ports 1-3:

```
DWS-3160-24PC:admin# clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3

Success.

DWS-3160-24PC:admin#
```

34-12 show address_binding dhcp_snoop

Description

This command is used to display the DHCP snooping configuration and learning database.

Format

show address_binding dhcp_snoop {max_entry {ports <portlist>}}

Parameters

max_entry - (Optional) To display the maximum number of entries per port.
  ports - Specifies the ports used for this configuration.
    <portlist> - Enter a list of ports used here.

If no parameters are specified, display DHCP snooping displays the enable/disable state.

Restrictions

None.

Example

To display the DHCP snooping state:

```
DWS-3160-24PC:admin#show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP Snoop(IPv4) : Enabled

DWS-3160-24PC:admin#
```

To display DHCP snooping maximum entry configuration:

```
DWS-3160-24PC:admin# show address_binding dhcp_snoop max_entry
Command: show address_binding dhcp_snoop max_entry

Port  Max Entry
----  ---------
1   No Limit
2   No Limit
3   No Limit
4   No Limit
5   No Limit
6   No Limit
7   No Limit
8   No Limit
9   No Limit
10  No Limit
11  No Limit
12  No Limit
13  No Limit
14  No Limit
15  No Limit
16  No Limit
17  No Limit
18  No Limit
19  No Limit
20  No Limit
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

34-13 show address_binding dhcp_snoop binding_entry

Description

This command is used to display the DHCP snooping binding entries.

Format

show address_binding dhcp_snoop binding_entry {port <port>}

Parameters

port – (Optional) Specifies the port used for this configuration.
  <port> - Enter the port number used here.

Restrictions

None.

Example

To display the DHCP snooping binding entries:

```
DWS-3160-24PC:admin#show address_binding dhcp_snoop binding_entry
Command: show address_binding dhcp_snoop binding_entry

 S (Status) - A: Active, I: Inactive
 Time - Left Time (sec)

 IP Address                              MAC Address       S  LT(sec)    Port
 --------------------------------------- ----------------- -- ---------- -----
 10.62.58.35                             00-0B-5D-05-34-0B A  35964      1
 10.33.53.82                             00-20-c3-56-b2-ef I  2590       2

Total entries : 2

DWS-3160-24PC:admin#
```

34-14 config address_binding dhcp_snoop max_entry

Description

This command is used to configure the maximum number of entries that can be learned by a specified port.

Format

config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-50> | no_limit]

Parameters

ports - Specifies the list of ports you would like to set the maximum number of entries that can be learned.
<portlist> - Enter the list of ports used here.
all - Specifies that all the ports will be used.

limit - Specifies the maximum number.
<value 1-50> - Enter the limit value here. This value must be between 1 and 50.
no_limit - Specifies that the maximum number of learned entries is unlimited.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the maximum number of DHCP IPv4 snooping entries that ports 1–3 can learn to 10:

```
DWS-3160-24PC:admin#config address_binding dhcp_snoop max_entry ports 1-3 limit
10
Command: config address_binding dhcp_snoop max_entry ports 1-3 limit 10

Success.

DWS-3160-24PC:admin#
```

34-15 enable address_binding trap_log

Description

This command is used to send traps and logs when the IMPB module detects an illegal IP and MAC address.

Format

enable address_binding trap_log

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the IMPB traps and logs:

```
DWS-3160-24PC:admin# enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DWS-3160-24PC:admin#
```

34-16 disable address_binding trap_log

Description

This command is used to disable the IMPB traps and logs.

Format

disable address_binding trap_log

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable IMPB traps and logs:

```
DWS-3160-24PC:admin# disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DWS-3160-24PC:admin#
```

34-17 config address_binding recover_learning

Description

This command is used to recover IMPB checking.

Format

config address_binding recover_learning ports [<portlist> | all]

Parameters

ports - Specifies the list of ports that need to recover the IMPB check.
  <portlist> - Enter the list of port used here.
  all - Specifies that all the ports will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To recover IMPB checking for ports 6 to 7:

```
DWS-3160-24PC:admin# config address_binding recover_learning ports 6-7
Command: config address_binding recover_learning ports 6-7

Success.

DWS-3160-24PC:admin#
```

Chapter 35 IPv6 Neighbor Discover Command List

create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>
delete ipv6 neighbor_cache ipif [<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]
show ipv6 neighbor_cache ipif [<ipif_name 12> **|** all] [ipv6address <ipv6addr> **|** static **|** dynamic **|** all]
config ipv6 nd ns ipif <ipif_name 12> **retrans_time** <millisecond 0-4294967295>
show ipv6 nd {ipif <ipif_name 12>}

35-1 create ipv6 neighbor_cache

Description

This command is used to create a static neighbor on an IPv6 interface.

Format

create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>

Parameters

ipif - Specifies the interface's name. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
<ipv6addr> - The address of the neighbor.
<macaddr> - The MAC address of the neighbor.

Restrictions

Only Administrators, Operators and Power-Users can issue this command. **)**

Example

Create a static neighbor cache entry:

```
DWS-3160-24PC:admin#create ipv6 neighbor_cache ipif System 3FFC::1 00-11-22-33-
44-55
Command: create ipv6 neighbor_cache ipif System 3FFC::1 00-11-22-33-44-55


Success.


DWS-3160-24PC:admin#
```

35-2 delete ipv6 neighbor_cache

Description

This command is used to delete a neighbor cached entry or static neighbor cache entries from the address cache or all address cache entries on this IP interface. Both static and dynamic entries can be deleted.

Format

delete ipv6 neighbor_cache ipif [<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]

Parameters

ipif - Specifies the IPv6 interface name.
- **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
- **all** - Specifies that all the interfaces will be used in this configuration.

<ipv6addr> - The neighbor’s address.

static - Delete the static entry.

dynamic - Delete those dynamic entries.

all - All entries include static and dynamic entries will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

Delete a neighbor cached entry on IP interface “System”:

```
DWS-3160-24PC:admin# delete ipv6 neighbor_cache ipif System 3ffc::1
Command: delete ipv6 neighbor_cache ipif System 3FFC::1

Success.

DWS-3160-24PC:admin#
```

35-3 show ipv6 neighbor_cache

Description

This command is used to display neighbor cached entries for the specified interface. You can display a specific entry, all entries, or all static entries.

Format

show ipv6 neighbor_cache ipif [<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic | all]

Parameters

ipif - Specifies the IPv6 interface name

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
all - Specifies that all the interface will be displayed.

ipv6address - The neighbor's address.
<ipv6addr> - Enter the IPv6 address here.

static - Static neighbor cache entry.

dynamic - Dynamic entries.

all - All entries include static and dynamic entries.

Restrictions

None

Example

Display all neighbor cache entries of IP interface "System":

```
DWS-3160-24PC:admin#show ipv6 neighbor_cache ipif System all
Command: show ipv6 neighbor_cache ipif System all

3FFC::1                                State: Static
MAC Address : 00-11-22-33-44-55        Port : NA
Interface   : System                   VID  : 1

Total Entries: 1

DWS-3160-24PC:admin#
```

35-4 config ipv6 nd ns retrans_time

Description

This command is used to configure the IPv6 ND neighbor solicitation retransmit time, which is between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reach ability of a neighbor.

Format

config ipv6 nd ns ipif <ipif_name 12> retrans_time <millisecond 0-4294967295>

Parameters

ipif - The IPv6 interface name
<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.

retrans_time - Neighbor solicitation's re-transmit timer in millisecond.
<millisecond 0-4294967295> - Enter the re-transmit timer value here. This value must be between 0 and 4294967295 milliseconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the retrans_time of IPv6 ND neighbor solicitation:

```
DWS-3160-24PC:admin#config ipv6 nd ns ipif System retrans_time 1000000
Command: config ipv6 nd ns ipif System retrans_time 1000000

Success.

DWS-3160-24PC:admin#
```

35-5 show ipv6 nd

Description

This command is used to display information regarding neighbor detection on the Switch.

Format

show ipv6 nd {ipif <ipif_name 12>}

Parameters

ipif – (Optional) The name of the interface. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
If no IP interface is specified, it will display the IPv6 ND related configuration of all interfaces.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To display IPv6 ND related configuration:

```
DWS-3160-24PC:admin#show ipv6 nd ipif System
Command: show ipv6 nd ipif System

Interface Name            : System
NS Retransmit Time        : 1000000 (ms)

DWS-3160-24PC:admin#
```

Chapter 36 IPv6 Route Command List

create ipv6route [default] [<ipif_name 12> <ipv6addr> |<ipv6addr>] {<metric 1-65535>} {[primary | backup]}
delete ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr> | all]
show ipv6route

36-1 create ipv6route

Description

This command is used to create an IPv6 default route. If the next hop is a global address, it is not needed to indicate the interface name. If the next hop is a link local address, then the interface name must be specified.

Format

create ipv6route [default] [<ipif_name 12> <ipv6addr> |<ipv6addr>] {<metric 1-65535>} {[primary | backup]}

Parameters

default - Specifies the default route.
<ipif_name 12> - Specifies the interface for the route. This name can be up to 12 characters long.
<ipv6addr> - Specifies the next hop address for this route.
<metric 1-65535> - Enter the metric value here. The default setting is 1. This value must between 1 and 65535.
primary - Specifies the route as the primary route to the destination. **backup** - Specifies the route as the backup route to the destination. The backup route can only be added when the primary route exists. If the route is not specified as the primary route or the backup route, then it will be auto-assigned by the system. The first created is the primary, the second created is the backup.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create and IPv6 route:

```
DWS-3160-24PC:admin# create ipv6route default System 3FFC:: 1 primary
Command: create ipv6route default System 3FFC:: 1 primary

Success.

DWS-3160-24PC:admin#
```

36-2 delete ipv6route

Description

This command is used to delete an IPv6 static route. If the next hop is a global address, it is not needed to indicate the interface name. If the next hop is a link local address, then the interface name must be specified.

Format

delete ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr> | all]

Parameters

default - Specifies the default route.

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

<ipv6addr> - Specifies the next hop address for the default route.

all - Specifies that all static created routes will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

Delete an IPv6 static route:

```
DWS-3160-24PC:admin# delete ipv6route default System 3FFC::
Command: delete ipv6route default System 3FFC::

Success.

DWS-3160-24PC:admin#
```

36-3 show ipv6route

Description

This command is used to display IPv6 routes.

Format

show ipv6route

Parameters

None.

Restrictions

None.

Example

Display all the IPv6 routes:

```
DWS-3160-24PC:admin#show ipv6route
Command: show ipv6route

IPv6 Prefix: ::/0                             Protocol: Static  Metric: 1
Next Hop   : 3001::254                        IPIF    : System
Backup     : Primary                          Status  : Inactive

Total Entries: 1

DWS-3160-24PC:admin#
```

Chapter 37 Jumbo Frame Command List

enable jumbo_frame

disable jumbo_frame

show jumbo_frame

37-1 enable jumbo_frame

Description

This command is used to configure the jumbo frame setting as enable.

Format

enable jumbo_frame

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the Jumbo frame:

```
DWS-3160-24PC:admin# enable jumbo_frame
Command: enable jumbo_frame

The maximum size of jumbo frame is 13312 bytes.
Success.

DWS-3160-24PC:admin#
```

37-2 disable jumbo_frame

Description

This command is used to configure the jumbo frame setting as disable.

Format

disable jumbo_frame

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the Jumbo frame:

```
DWS-3160-24PC:admin# disable jumbo_frame
Command: disable jumbo_frame

Success.

DWS-3160-24PC:admin#
```

37-3 show jumbo_frame

Description

This command is used to display the current configuration of jumbo frame.

Format

show jumbo_frame

Parameters

None.

Restrictions

None.

Example

To display the Jumbo frame:

```
DWS-3160-24PC:admin#show jumbo_frame
Command: show jumbo_frame

Jumbo Frame State  : Enabled
Maximum Jumbo Frame Size : 13312 Bytes

DWS-3160-24PC:admin#
```

Chapter 38 Link Aggregation Command List

create link_aggregation group_id <value 1-32> {type [lacp | static]}

delete link_aggregation group_id <value 1-32>

config link_aggregation group_id <value 1-32> {master_port <port> | ports <portlist> | state [enabled | disabled]}

config link_aggregation algorithm [mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest | l4_src_port | l4_dest_port | l4_src_dest_port]

show link_aggregation {group_id <value 1-32> | algorithm}

config lacp_port <portlist> mode [active | passive]

show lacp_port <portlist>

38-1 create link_aggregation group_id

Description

This command is used to create a link aggregation group on the Switch.

Format

create link_aggregation group_id <value 1-32> {type [lacp | static]}

Parameters

group_id - Specifies the group id. The group number identifies each of the groups.
<value 1-32> - Enter the group ID value here. This value must be between 1 and 32.

type - (Optional) Specifies the group type that belongs to static or LACP. If type is not specified, the default is static type.
lacp - Specifies to use LACP as the group type.
static - Specifies to use static as the group type.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create link aggregation group:

```
DWS-3160-24PC:admin# create link_aggregation group_id 1 type lacp
Command: create link_aggregation group_id 1 type lacp

Success.

DWS-3160-24PC:admin#
```

38-2 delete link_aggregation group_id

Description

This command is used to delete a configured link aggregation group.

Format

delete link_aggregation group_id <value 1-32>

Parameters

group_id - Specifies the group id. The group number identifies each of the groups.
<value 1-32> - Enter the group ID value here. This value must be between 1 and 32.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete link aggregation group:

```
DWS-3160-24PC:admin# delete link_aggregation group_id 3
Command: delete link_aggregation group_id 3

Success.

DWS-3160-24PC:admin#
```

38-3 config link_aggregation

Description

This command is used to configure a link aggregation group.

Format

config link_aggregation group_id <value 1-32> {master_port <port> | ports <portlist> | state [enabled | disabled]}

Parameters

group_id - Specifies the group id. The group number identifies each of the groups.
<value 1-32> - Enter the group ID value here. This value must be between 1 and 32.

master_port - (Optional) Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port.
<port> - Enter the master port number here.

ports - (Optional) Specifies a range of ports that will belong to the link aggregation group. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then highest Switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash.

<portlist> - Enter the list of port used for the configuration here.

state - (Optional) Allows you to enable or disable the specified link aggregation group. If not specified, the group will keep the previous state, the default state is disabled. If configure LACP group, the ports' state machine will start.
enable - Enables the specified link aggregation group.
disable - Disables the specified link aggregation group.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To define a load-sharing group of ports, group-id 1, master port 17:

```
DWS-3160-24PC:admin# config link_aggregation group_id 1 master_port 17 ports 5-
10,17
command: config link_aggregation group_id 1 master_port 17 ports 5-10,17

Success.

DWS-3160-24PC:admin#
```

38-4 config link_aggregation algorithm

Description

This command is used to configure the part of the packet examined by the Switch when selecting the egress port for transmitting load-sharing data. This feature is available using the address-based load-sharing algorithm, only.

Format

config link_aggregation algorithm [mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest | l4_src_port | l4_dest_port | l4_src_dest_port]

Parameters

mac_source - Indicates that the Switch should examine the MAC source address.

mac_destination - Indicates that the Switch should examine the MAC destination address.

mac_source_dest - Indicates that the Switch should examine the MAC source and destination address.

ip_source - Indicates that the Switch should examine the IP source address.

ip_destination - Indicates that the Switch should examine the IP destination address.

ip_source_dest - Indicates that the Switch should examine the IP source address and destination address.

l4_src_port - Indicates that the Switch should examine the TCP/UDP source port.

l4_dest_port - Indicates that the Switch should examine the TCP/UDP destination port.

l4_src_dest_port - Indicates that the Switch should examine the TCP/UDP source port and destination port.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure link aggregation algorithm for MAC-Source-Dest:

```
DWS-3160-24PC:admin# config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DWS-3160-24PC:admin#
```

38-5 show link_aggregation

Description

This command is used to display the current link aggregation configuration on the Switch.

Format

show link_aggregation {group_id <value 1-32> | algorithm}

Parameters

group_id - (Optional) Specifies the group id. The group number identifies each of the groups.
<value 1-32> - Enter the group ID value here. This value must be between 1 and 32.

algorithm - (Optional) Allows you to Specifies the display of link aggregation by the algorithm in use by that group.

If no parameter specified, system will display all link aggregation information.

Restrictions

None.

Example

Link aggregation group enable:

```
DWS-3160-24PC:admin# show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest

Group ID      : 1
Type          : LACP
Master Port   : 1
Member Port   : 1-8
Active Port   : 7
Status        : Enabled
Flooding Port : 7

Total Entries : 1

DWS-3160-24PC:admin#
```

Link aggregation group enable and no member linkup:

```
DWS-3160-24PC:admin# show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest

Group ID      : 1
Type          : LACP
Master Port   : 1
Member Port   : 1-8
Active Port   :
Status        : Enabled
Flooding Port :

Total Entries : 1

DWS-3160-24PC:admin#
```

Link aggregation group disabled:

```
DWS-3160-24PC:admin# show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest

Group ID      : 1
Type          : LACP
Master Port   : 1
Member Port   : 1-8
Active Port   :
Status        : Disabled
Flooding Port :

Total Entries : 1

DWS-3160-24PC:admin#
```

38-6 config lacp_port

Description

This command is used to configure the per-port LACP mode.

Format

config lacp_port <portlist> mode [active | passive]

Parameters

lacp_port - Specified a range of ports to be configured. **<portlist>** - Enter the list of port used for the configuration here.
mode - Specifies the LACP mode used. **active** - Specifies to set the LACP mode as active. **passive -** Specifies to set the LACP mode as passive.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To config port LACP mode:

```
DWS-3160-24PC:admin# config lacp_port 1-12 mode active
command: config lacp_port 1-12 mode active

Success.

DWS-3160-24PC:admin#
```

38-7 show lacp_port

Description

This command is used to display the current mode of LACP of the ports.

Format

show lacp_port <portlist>

Parameters

lacp_port - Specified a range of ports to be configured.

  <portlist> - Enter the list of ports used for this configuration here.

If no parameter specified, the system will display current LACP and all port status.

Restrictions

None.

Example

To display port lacp mode:

```
DWS-3160-24PC:admin#show lacp_port
Command: show lacp_port

 Port     Activity
 -----    --------
 1        Active
 2        Active
 3        Active
 4        Active
 5        Active
 6        Active
 7        Active
 8        Active
 9        Active
 10       Active
 11       Active
 12       Active
 13       Passive
 14       Passive
 15       Passive
 16       Passive
 17       Passive
 18       Passive
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Chapter 39 Link Layer Discovery Protocol (LLDP) Command List

enable lldp
disable lldp
config lldp [message_tx_interval <sec 5-32768> | message_tx_hold_multiplier <int 2-10> | tx_delay <sec 1-8192> | reinit_delay <sec 1-10>]
config lldp notification_interval <sec 5-3600>
config lldp ports [<portlist> | all] [notification [enable | disable] | admin_status [tx_only | rx_only | tx_and_rx | disable] | mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] [enable | disable] | basic_tlvs [{all} | {port_description | system_name | system_description | system_capabilities}] [enable | disable] | dot1_tlv_pvid [enable | disable] | dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp}] [enable | disable] | dot3_tlvs [{all} | {mac_phy_configuration_status | link_aggregation | power_via_mdi | maximum_frame_size}] [enable | disable]]
config lldp forward_message [enable | disable]
show lldp
show lldp mgt_addr {ipv4 <ipaddr> | ipv6 <ipv6addr>}
show lldp ports {<portlist>}
show lldp local_ports {<portlist>} {mode [brief | normal | detailed]}
show lldp remote_ports {<portlist>} [brief | normal | detailed]
show lldp statistics
show lldp statistics ports {<portlist>}

39-1 enable lldp

Description

This command is used to globally enable the LLDP function.

When this function is enabled, the Switch can start to transmit LLDP packets and receive and process the LLDP packets. The specific function of each port will depend on the per-port LLDP setting.

For the advertisement of LLDP packets, the Switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the Switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table. The default state for LLDP is disabled.

Format

enable lldp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable LLDP:

```
DWS-3160-24PC:admin# enable lldp
Command: enable lldp

Success.

DWS-3160-24PC:admin#
```

39-2 disable lldp

Description

This command is used to globally disable the LLDP function.

Format

disable lldp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable LLDP:

```
DWS-3160-24PC:admin# disable lldp
Command: disable lldp

Success.

DWS-3160-24PC:admin#
```

39-3 config lldp

Description

This command is used to change the packet transmission interval.

Format

config lldp [message_tx_interval <sec 5-32768> | message_tx_hold_multiplier <int 2-10> | tx_delay <sec 1-8192> | reinit_delay <sec 1-10>]

Parameters

message_tx_interval - Changes the interval between consecutive transmissions of LLDP advertisements on any given port. The default setting 30 seconds.
<sec 5-32768> - Enter the message transmit interval value here. This value must be between 5 and 32768 seconds.

message_tx_hold_multiplier - Specifies to configure the message hold multiplier. The default setting 4.
<2-10> - Enter the message transmit hold multiplier value here. This value must be between 2 and 10.

tx_delay - Specifies the minimum interval between sending of LLDP messages due to constantly change of MIB content. The default setting 2 seconds.
<sec 1-8192> - Enter the transmit delay value here. This value must be between 1 and 8192 seconds.

reinit_delay - Specifies the minimum time of re-initialization delay interval. The default setting 2 seconds.
<sec 1-10> - Enter the re-initiate delay value here. This value must be between 1 and 10 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To change the packet transmission interval:

```
DWS-3160-24PC:admin# config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

DWS-3160-24PC:admin#
```

39-4 config lldp notification_interval

Description

This command is used to configure the timer of notification interval for sending notification to configured SNMP trap receiver(s).

Format

config lldp notification_interval <sec 5-3600>

Parameters

notification_interval - Specifies the timer of notification interval for sending notification to configured SNMP trap receiver(s). The default setting is 5 seconds.

<sec 5-3600> - Enter the notification interval value here. This value must be between 5 and 3600 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To changes the notification interval to 10 second:

```
DWS-3160-24PC:admin# config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

DWS-3160-24PC:admin#
```

39-5 config lldp ports

Description

This command is used to configure each port for sending a notification to configure the SNMP trap receiver(s).

Format

config lldp ports [<portlist> | all] [notification [enable | disable] | admin_status [tx_only | rx_only | tx_and_rx | disable] | mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] [enable | disable] | basic_tlvs [{all} | {port_description | system_name | system_description | system_capabilities}] [enable | disable] | dot1_tlv_pvid [enable | disable] | dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp}] [enable | disable] | dot3_tlvs [{all} | {mac_phy_configuration_status | link_aggregation | power_via_mdi | maximum_frame_size}] [enable | disable]]

Parameters

<portlist> - Enter a list of ports used for the configuration here.

all - Specifies that all the ports will be used for this configuration.

notification - Enables or disables the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices. The default notification state is disabled.

- **enable** - Specifies that the SNMP trap notification of LLDP data changes detected will be enabled.
- **disable** - Specifies that the SNMP trap notification of LLDP data changes detected will be disabled.

admin_status - Specifies the per-port transmit and receive modes.

- **tx_only** - Configure the specified port(s) to transmit LLDP packets, but block inbound LLDP packets from neighbor devices.
- **rx_only** - Configure the specified port(s) to receive LLDP packets from neighbors, but block outbound packets to neighbors.
- **tx_and_rx** - Configure the specified port(s) to both transmit and receive LLDP packets.
- **disable** - Disable LLDP packet transmit and receive on the specified port(s).

mgt_addr - Specifies the management address used.
  ipv4 - Specifies the IPv4 address used.
    <ipaddr> - Enter the IP address used for this configuration here.
  ipv6 - Specifies the IPv6 address used.
    <ipv6addr> - Enter the IPv6 address used for this configuration here.

enable - Specifies that the advertising indicated management address instance will be enabled.
disable - Specifies that the advertising indicated management address instance will be disabled.

basic_tlvs - Specifies the basic TLV data types used from outbound LLDP advertisements.
  all - Specifies that all the basic TLV data types will be used.
  port_description - (Optional) This TLV optional data type indicates that LLDP agent should transmit 'Port Description TLV on the port. The default state is disabled.
  system_name - (Optional) This TLV optional data type includes indicates that LLDP agent should transmit 'System Name TLV'. The default state is disabled.
  system_description - (Optional) This TLV optional data type includes indicates that LLDP agent should transmit 'System Description TLV'. The default state is disabled.
  system_capabilities - (Optional) This TLV optional data type includes indicates that LLDP agent should transmit 'System Capabilities TLV'. The system capability will indicate whether the device provides repeater, bridge, or router function, and whether the provided functions are currently enabled. The default state is disabled.

enable - Specifies that the basic TLV data types used from outbound LLDP advertisements will be enabled.
disable - Specifies that the basic TLV data types used from outbound LLDP advertisements will be disabled.

dot1_tlv_pvid - This TLV optional data type determines whether the IEEE 802.1 organizationally defined port VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.

enable - Specifies that the Dot1 TLV PVID option will be enabled.
disable - Specifies that the Dot1 TLV PVID option will be disabled.

dot1_tlv_protocol_vid - This TLV optional data type determines whether the IEEE 802.1 organizationally defined port and protocol VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.

vlan - Specifies the VLAN used for this configuration.
  all - Specifies that all the configured VLANs will be used for this configuration.
  <vlan_name 32> - Enter the name of the VLAN here. This name can be up to 32 characters long.
  vlanid - Specifies the VLAN ID used for this configuration.
    <vlanid_list> - Enter the ID of the VLAN here.

enable - Specifies that the Dot1 TLV protocol VID will be enabled.
disable - Specifies that the Dot1 TLV protocol VID will be disabled.

dot1_tlv_vlan_name - This TLV optional data type indicates whether the corresponding Local System’s VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs. those enabled VLAN ID will be advertised. The default state is disabled.

vlan - Specifies the VLAN used for this configuration.
  all - Specifies that all the configured VLANs will be used for this configuration.
  <vlan_name 32> - Enter the name of the VLAN here. This name can be up to 32 characters long.
  vlanid - Specifies the VLAN ID used for this configuration.
    <vlanid_list> - Enter the ID of the VLAN here.

enable - Specifies that the Dot1 TLV VLAN name will be enabled.
disable - Specifies that the Dot1 TLV VLAN name will be disabled.

dot1_tlv_protocol_identity - This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP (including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised. The default state is disabled.
  all - Specifies that all the vendor proprietary protocols will be advertised.

eapol - (Optional) Specifies that the EAPOL protocol will be advertised.
lacp - (Optional) Specifies that the LACP protocol will be advertised.
gvrp - (Optional) Specifies that the GVRP protocol will be advertised.
stp - (Optional) Specifies that the STP protocol will be advertised.

enable - Specifies that the protocol identity TLV according to the protocol specified will be advertised.
disable - Specifies that the protocol identity TLV according to the protocol specified will not be advertised.

dot3_tlvs - Specifies that the IEEE 802.3 specific TLV data type will be configured.
a**ll** - Specifies that all the IEEE 802.3 specific TLV data type will be used.
mac_phy_configuration_status - (Optional) This TLV optional data type indicates that LLDP agent should transmit 'MAC/PHY configuration/status TLV'. This type indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port supported the auto-negotiation function, whether the function is enabled, the auto-negotiated advertised capability, and the operational MAU type. The default state is disabled.
link_aggregation - (Optional) This TLV optional data type indicates that LLDP agent should transmit 'Link Aggregation TLV'. This type indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in a aggregated link, and the aggregated port ID. The default state is disabled.
power_via_mdi - (Optional) This TLV optional data type indicates that LLDP agent should transmit 'Power via MDI TLV'. Three IEEE 802.3 PMD implementations (10BASE-T, 100BASE-TX, and 1000BASE-T) allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station. The default state is disabled.
maximum_frame_size - (Optional) This TLV optional data type indicates that LLDP agent should transmit 'Maximum-frame-size TLV. The default state is disabled.

enable - Specifies that the IEEE 802.3 specific TLV data type selected will be advertised.
disable - Specifies that the IEEE 802.3 specific TLV data type selected will be not advertised.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable SNMP notifications from port 1-5:

```
DWS-3160-24PC:admin# config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

DWS-3160-24PC:admin#
```

To configure port 1-5 to transmit and receive:

```
DWS-3160-24PC:admin# config lldp ports 1-5 admin_status tx_and_rx
Command: config lldp ports 1-5 admin_status tx_and_rx

Success.

DWS-3160-24PC:admin#
```

To enable ports 1-2 for manage address entry:

```
DWS-3160-24PC:admin#config lldp ports 5-6 mgt_addr ipv4 10.90.90.90 enable
Command: config lldp ports 5-6 mgt_addr ipv4 10.90.90.90 enable

Success.

DWS-3160-24PC:admin#
```

To configure exclude the system name TLV from the outbound LLDP advertisements for all ports:

```
DWS-3160-24PC:admin# config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

DWS-3160-24PC:admin#
```

To configure exclude the vlan nameTLV from the outbound LLDP advertisements for all ports:

```
DWS-3160-24PC:admin# config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

DWS-3160-24PC:admin#
```

To configure exclude the port and protocol VLAN ID TLV from the outbound LLDP advertisements for all ports:

```
DWS-3160-24PC:admin# config lldp ports all dot1_tlv_protocol_vid vlanid 1-3
enable
Command: config lldp ports all dot1_tlv_protocol_vid vlanid 1-3 enable

Success.

DWS-3160-24PC:admin#
```

To configure exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DWS-3160-24PC:admin# config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable
Command: config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable

Success.

DWS-3160-24PC:admin#
```

To configure exclude the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
DWS-3160-24PC:admin# config lldp ports all dot1_tlv_protocol_identity all
enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

DWS-3160-24PC:admin#
```

To configure exclude the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

```
DWS-3160-24PC:admin# config lldp ports all dot3_tlvs
mac_phy_configuration_status enable
Command: config lldp ports all dot3_tlvs mac_phy_configuration_status enable

Success.

DWS-3160-24PC:admin#
```

39-6 config lldp forward_ message

Description

This command is used to configure forwarding of LLDP PDU packets when LLDP is disabled.

Format

config lldp forward_message [enable | disable]

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure LLDP to forward LLDP PDUs:

```
DWS-3160-24PC:admin# config lldp forward_message enable
Command: config lldp forward_message enable

Success.

DWS-3160-24PC:admin#
```

39-7 show lldp

Description

This command is used to display the Switch’s general LLDP configuration status.

Format

show lldp

Parameters

None.

Restrictions

None.

Example

To display the LLDP system level configuration status:

```
DWS-3160-24PC:admin#show lldp
Command: show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address
    Chassis ID                : 00-11-22-33-45-67
    System Name               :
    System Description        : Gigabit Ethernet Switch
    System Capabilities       : Repeater, Bridge

LLDP Configurations
    LLDP Status               : Enabled
    LLDP Forward Status       : Enabled
    Message TX Interval       : 30
    Message TX Hold Multiplier: 4
    ReInit Delay              : 2
    TX Delay                  : 2
    Notification Interval     : 10

DWS-3160-24PC:admin#
```

39-8 show lldp mgt_addr

Description

This command is used to display the LLDP management address information.

Format

show lldp mgt_addr {ipv4 <ipaddr> | ipv6 <ipv6addr>}

Parameters

ipv4 - (Optional) Specifies the IPv4 address used for the display. **<ipaddr>** - Enter the IPv4 address used for this configuration here.

ipv6 - (Optional) Specifies the IPv6 address used for the display.
<ipv6addr> - Enter the IPv6 address used for this configuration here.

Restrictions

None.

Example

To display management address information:

```
DWS-3160-24PC:admin#show lldp mgt_addr ipv4 10.90.90.90
Command: show lldp mgt_addr ipv4 10.90.90.90

Address 1 :
------------------------------------------------
    Subtype                            : IPv4
    Address                            : 10.90.90.90
    IF Type                            : IfIndex
    OID                                : 1.3.6.1.4.1.171.11.124.2
    Advertising Ports                  : 5-6

DWS-3160-24PC:admin#
```

39-9 show lldp ports

Description

This command is used to display the LLDP per port configuration for advertisement options.

Format

show lldp ports {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be displayed.
If the port list is not specified, information for all the ports will be displayed.

Restrictions

None.

Example

To display the LLDP port 5 TLV option configuration:

```
DWS-3160-24PC:admin#show lldp ports 5
Command: show lldp ports 5

Port ID                 : 5
-----------------------------------------------------------------
Admin Status            : TX_and_RX
Notification Status     : Enabled
Advertised TLVs Option  :
    Port Description                                      Disabled
    System Name                                           Enabled
    System Description                                    Disabled
    System Capabilities                                   Disabled
    Enabled Management Address
        10.90.90.90
    Port VLAN ID                                          Enabled
    Enabled Port_and_Protocol_VLAN_ID
        1, 2, 3
    Enabled VLAN Name
        1-3
    Enabled Protocol_Identity
        EAPOL, LACP, GVRP, STP
    MAC/PHY Configuration/Status                          Enabled
    Power Via MDI                                         Disabled
    Link Aggregation                                      Disabled
    Maximum Frame Size                                    Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

39-10 show lldp local_ports

Description

This command is used to display the per-port information currently available for populating outbound LLDP advertisements.

Format

show lldp local_ports {<portlist>} {mode [brief | normal | detailed]}

Parameters

<portlist> - (Optional) Specified a range of ports to be configured. When port list is not specified, information for all ports will be displayed.	
mode - (Optional) Specifies the display mode. **brief** - Display the information in brief mode. **normal** - Display the information in normal mode. This is the default display mode. **detailed** - Display the information in detailed mode.	

Restrictions

None.

Example

To display outbound LLDP advertisements for port 1 in detailed mode. Port description on the display should use the same value as ‘ifDescr’.

```
DWS-3160-24PC:admin#show lldp local_ports 1 mode detailed
Command: show lldp local_ports 1 mode detailed

Port ID : 1
-----------------------------------------------------------------------------
Port ID Subtype                            : Local
Port ID                                    : 1/1
Port Description                           : D-Link DWS-3160-24PC R1.00.034
                                             Port 1
Port PVID                                  : 1
Management Address Count                   : 1
        Subtype                            : IPv4
        Address                            : 192.168.69.123
        IF Type                            : IfIndex
        OID                                : 1.3.6.1.4.1.171.10.117.1.2

PPVID Entries Count                        : 0
    (None)
VLAN Name Entries Count                    : 1
    Entry 1 :
        VLAN ID                            : 1
        VLAN Name                          : default

Protocol Identity Entries Count            : 0
    (None)
MAC/PHY Configuration/Status               :
    Auto-Negotiation Support               : Supported
    Auto-Negotiation Enabled               : Enabled
    Auto-Negotiation Advertised Capability : 6c01(hex)
    Auto-Negotiation Operational MAU Type  : 0000(hex)

Power Via MDI                              :
    Port Class                             : PSE
    PSE MDI Power Support                  : Supported
    PSE MDI Power State                    : Enabled
    PSE Pairs Control Ability              : Uncontrollable
    PSE Power Pair                         : 1
    Power Class                            : 1
    Power Type                             : Type 2 PSE
    Power Source                           : Primary power source
    Power Priority                         : low
    PD requested power                     : 0
    PSE allocated power                    : 0

Link Aggregation                           :
    Aggregation Capability                 : Aggregated
    Aggregation Status                     : Not Currently in Aggregation
    Aggregation Port ID                    : 0
```

```
Maximum Frame Size                          : 1542

DWS-3160-24PC:admin#
```

To display outbound LLDP advertisements for port 1 in normal mode:

```
DWS-3160-24PC:admin#show lldp local_ports 1 mode normal
Command: show lldp local_ports 1 mode normal

Port ID : 1
-----------------------------------------------------------------------------
Port ID Subtype                             : Local
Port ID                                     : 1/1
Port Description                            : D-Link DWS-3160-24PC R1.00.034
                                              Port 1
Port PVID                                   : 1
Management Address Count                    : 1
PPVID Entries Count                         : 0
VLAN Name Entries Count                     : 1
Protocol Identity Entries Count             : 0
MAC/PHY Configuration/Status                : (See Detail)
Power Via MDI                               : (See Detail)
Link Aggregation                            : (See Detail)
Maximum Frame Size                          : 1542

DWS-3160-24PC:admin#
```

To display outbound LLDP advertisements for port 1 in brief mode:

```
DWS-3160-24PC:admin#show lldp local_ports 1 mode brief
Command: show lldp local_ports 1 mode brief


Port ID : 1
-----------------------------------------------------------------------------
Port ID Subtype                             : Local
Port ID                                     : 1/1
Port Description                            : D-Link DWS-3160-24PC R1.00.034
                                              Port 1

DWS-3160-24PC:admin#
```

39-11 show lldp remote_ports

Description

This command is used to display the information learned from the neighbor parameters.

Format

show lldp remote_ports {<portlist>} [brief | normal | detailed]

Parameters

<portlist> - (Optional) Specified a range of ports to be configured. When port list is not specified, information for all ports will be displayed.

brief - (Optional) Display the information in brief mode.
normal - Display the information in normal mode. This is the default display mode.
detailed - Display the information in detailed mode.

Restrictions

None.

Example

To display remote table in brief mode:

```
DWS-3160-24PC:admin#show lldp remote_ports 23 mode brief
Command: show lldp remote_ports 23 mode brief

Port ID : 23
--------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                         : MAC Address
    Chassis ID                                 : 00-11-22-33-32-32
    Port ID Subtype                            : Local
    Port ID                                    : 1/23
    Port Description                           : D-Link DWS-3160-24TC R1.00.034
                                                 Port 23


DWS-3160-24PC:admin#
```

To display remote table in normal mode:

```
DWS-3160-24PC:admin#show lldp remote_ports 23 mode normal
Command: show lldp remote_ports 23 mode normal

Port ID : 23
--------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                         : MAC Address
    Chassis ID                                 : 00-11-22-33-32-32
    Port ID Subtype                            : Local
    Port ID                                    : 1/23
    Port Description                           : D-Link DWS-3160-24TC R1.00.034
                                                 Port 23
    System Name                                :
    System Description                         : Gigabit Ethernet Switch
    System Capabilities                        : Repeater, Bridge
    Management Address Count                   : 0
    Port PVID                                  : 0
    PPVID Entries Count                        : 0
    VLAN Name Entries Count                    : 0
    Protocol ID Entries Count                  : 0
    MAC/PHY Configuration/Status               : (None)
    Power Via MDI                              : (None)
    Link Aggregation                           : (None)
    Maximum Frame Size                         : 0
    Unknown TLVs Count                         : 0


DWS-3160-24PC:admin#
```

To display remote table in detailed mode:

```
DWS-3160-24PC:admin#show lldp remote_ports 23 mode detailed
Command: show lldp remote_ports 23 mode detailed

Port ID : 23
-------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                         : MAC Address
    Chassis ID                                 : 00-11-22-33-32-32
    Port ID Subtype                            : Local
    Port ID                                    : 1/23
    Port Description                           : D-Link DWS-3160-24TC R1.00.034
                                                 Port 23
    System Name                                :
    System Description                         : Gigabit Ethernet Switch
    System Capabilities                        : Repeater, Bridge
    Management Address Count                   : 0
        (None)

    Port PVID                                  : 0
    PPVID Entries Count                        : 0
        (None)

    VLAN Name Entries Count                    : 0
        (None)

    Protocol ID Entries Count                  : 0
        (None)

    MAC/PHY Configuration/Status               : (None)
    Power Via MDI                              : (None)
    Link Aggregation                           : (None)
    Maximum Frame Size                         : 0
    Unknown TLVs Count                         : 0
        (None)

DWS-3160-24PC:admin#
```

39-12 show lldp statistics

Description

This command is used to display an overview of neighbor detection activity on the Switch.

Format

show lldp statistics

Parameters

None.

Restrictions

None.

Example

To display global statistics information:

```
DWS-3160-24PC:admin#show lldp statistics
Command: show lldp statistics

Last Change Time       : 40600
Number of Table Insert : 1
Number of Table Delete : 0
Number of Table Drop   : 0
Number of Table Ageout : 0

DWS-3160-24PC:admin#
```

39-13 show lldp statistics ports

Description

This command is used to display per-port LLDP statistics.

Format

show lldp statistics ports {<portlist>}

Parameters

<portlist> - (Optional) Specified a range of ports to be configured. When port list is not specified, information for all ports will be displayed.

Restrictions

None.

Example

To display statistics information of port 1:

```
DWS-3160-24PC:admin#show lldp statistics ports 1
Command: show lldp statistics ports 1

Port ID : 1
---------------------------------------------
    LLDPStatsTXPortFramesTotal           : 22
    LLDPStatsRXPortFramesDiscardedTotal  : 0
    LLDPStatsRXPortFramesErrors          : 0
    LLDPStatsRXPortFramesTotal           : 0
    LLDPStatsRXPortTLVsDiscardedTotal    : 0
    LLDPStatsRXPortTLVsUnrecognizedTotal : 0
    LLDPStatsRXPortAgeoutsTotal          : 0

DWS-3160-24PC:admin#
```

Chapter 40 Loop Back Detection (LBD) Command List

config loopdetect {recover_timer [<value 0> | <sec 60-1000000>] | interval <sec 1-32767> | mode [port-based | vlan-based]}
config loopdetect ports [<portlist> | all] state [enable | disable]
enable loopdetect
disable loopdetect
show loopdetect
show loopdetect ports {<portlist>}
config loopdetect trap [none | loop_detected | loop_cleared | both]
config loopdetect log state [enable | disable]

40-1 config loopdetect

Description

This command is used to configure the Loop-back Detection (LBD) function.

Format

config loopdetect {recover_timer [<value 0> | <sec 60-1000000>] | interval <sec 1-32767> | mode [port-based | vlan-based]}

Parameters

recover_timer - (Optional) The time interval (in seconds) used by the Auto-Recovery mechanism to decide how long to check before determining that the loop status has gone. The valid range is from 60 to 1000000. 0 is a special value that specifies that the auto-recovery mechanism should be disabled. When the auto-recovery mechanism is disabled, a user would need to manually recover a disabled port. The default value for the recover timer is 60 seconds. **<value 0>** - 0 is a special value that specifies that the auto-recovery mechanism should be disabled. When the auto-recovery mechanism is disabled, a user would need to manually recover a disabled port. **<sec 60-1000000>** - Enter the recovery timer value here. This value must be between 60 and 1000000 seconds.
interval - (Optional) The time interval (in seconds) that the device will transmit all the CTP (Configuration Test Protocol) packets to detect a loop-back event. The default setting is 10 seconds. The valid range is from 1 to 32767 seconds. **<sec - 1-32767>** - Enter the time interval value here. This value must be between 1 and 32767 seconds.
mode - (Optional) Specifies the loop-detection operation mode. In port-based mode, the port will be shut down (disabled) when loop has been detected In VLAN-based mode, the port cannot process the packets of the VLAN that has detected the loop. **port-based** - Specifies that the loop-detection operation mode will be set to port-based mode. **vlan-based** - Specifies that the loop-detection operation mode will be set to vlan-based mode.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the auto-recover time to 0, which disables the auto-recovery mechanism, the interval to 20 seconds and Specifies VLAN-based mode:

```
DWS-3160-24PC:admin# config loopdetect recover_timer 0 interval 20 mode vlan-
based
Command: config loopdetect recover_timer 0 interval 20 mode vlan-based

Success.

DWS-3160-24PC:admin#
```

40-2 config loopdetect ports

Description

This command is used to configure the LBD function for interfaces on the Switch.

Format

config loopdetect ports [<portlist> | all] state [enable | disable]

Parameters

ports - Specifies the range of ports that LBD will be configured on.
<portlist> - Enter a list of ports
all - To set all ports in the system, you may use the "all" parameter.

state - Specifies whether the LBD function should be enabled or disabled on the ports specified in the port list. The default state is disabled.
enable - Specifies to enable the LBD function.
disable - Specifies to disable the LBD function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the LBD function on ports 1-5:

```
DWS-3160-24PC:admin# config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success.

DWS-3160-24PC:admin#
```

40-3 enable loopdetect

Description

This command is used to enable the LBD function globally on the Switch. The default state is disabled.

Format

enable loopdetect

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the LBD function globally:

```
DWS-3160-24PC:admin# enable loopdetect
Command: enable loopdetect

Success.

DWS-3160-24PC:admin#
```

40-4 disable loopdetect

Description

This command is used to disable the LBD function globally on the Switch.

Format

disable loopdetect

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the LBD function globally:

```
DWS-3160-24PC:admin# disable loopdetect
Command: disable loopdetect

Success.

DWS-3160-24PC:admin#
```

40-5 show loopdetect

Description

This command is used to display the LBD global configuration.

Format

show loopdetect

Parameters

None.

Restrictions

None.

Example

To display the LBD global settings:

```
DWS-3160-24PC:admin#show loopdetect
Command: show loopdetect

 LBD Global Settings
 ---------------------------
 Status         : Disabled
 Mode           : VLAN-based
 Interval       : 20 sec
 Recover Time   : 0 sec
 Trap State     : None
 Log State      : Enabled


DWS-3160-24PC:admin#
```

40-6 show loopdetect ports

Description

This command is used to display the LBD per-port configuration.

Format

show loopdetect ports {<portlist>}

Parameters

ports - Specifies the range of member ports that will display the LBD settings. **<portlist>** - Enter the list of port to be configured here.
If no port is specified, the configuration for all ports will be displayed.

Restrictions

None.

Example

To display the LBD settings on ports 1-9:

```
DWS-3160-24PC:admin#show loopdetect ports 1-9
Command: show loopdetect ports 1-9

Port   Loopdetect State    Loop VLAN
------ ----------------- ----------
1      Enabled             None
2      Enabled             None
3      Enabled             None
4      Enabled             None
5      Enabled             None
6      Disabled            None
7      Disabled            None
8      Disabled            None
9      Disabled            None

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

40-7 config loopdetect trap

Description

This command is used to configure the trap modes for LBD.

Format

config loopdetect trap [none | loop_detected | loop_cleared | both]

Parameters

none - There is no trap in the LBD function.
loop_detected - Trap will only be sent when the loop condition is detected.
loop_cleared - Trap will only be sent when the loop condition is cleared.
both - Trap will either be sent when the loop condition is detected or cleared.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To Specifies that traps will be sent when the loop condition is detected or cleared:

```
DWS-3160-24PC:admin# config loopdetect trap both
Command: config loopdetect trap both

Success.

DWS-3160-24PC:admin#
```

40-8 config loopdetect log

Description

This command is used to configure the log state for LBD. The default value is enabled.

Format

config loopdetect log state [enable | disable]

Parameters

state - Specifies the state of the LBD log feature.
- **enable** - Enable the LBD log feature.
- **disable** - Disable the LBD log feature. All LBD-related logs will not be recorded.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the log state for LBD:

```
DWS-3160-24PC:admin# config loopdetect log state enable
Command: config loopdetect log state enable

Success.

DWS-3160-24PC:admin#
```

Chapter 41 MAC Notification Command List

enable mac_notification

disable mac_notification

config mac_notification {interval <int 1-2147483647> **|** historysize <int 1-500>}

config mac_notification ports [<portlist> | all] [enable | disable]

show mac_notification

show mac_notification ports {<portlist>}

41-1 enable mac_notification

Description

This command is used to globally enable MAC address table notification on the Switch.

Format

enable mac_notification

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable mac_notification function:

```
DWS-3160-24PC:admin# enable mac_notification
Command: enable mac_notification

Success.

DWS-3160-24PC:admin#
```

41-2 disable mac_notification

Description

This command is used to globally disable MAC address table notification on the Switch.

Format

disable mac_notification

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable mac_notification function:

```
DWS-3160-24PC:admin# disable mac_notification
Command: disable mac_notification

Success.

DWS-3160-24PC:admin#
```

41-3 config mac_notification

Description

This command is used to configure the Switch’s MAC address table notification global settings.

Format

config mac_notification {interval <int 1-2147483647> | historysize <int 1-500>}

Parameters

interval - (Optional) The time in seconds between notifications.
<int 1-2147483647> - Enter the interval time here. This value must be between 1 and 2147483647 seconds.

historysize - (Optional) This is maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified.
<int 1-500> - Enter the history log size here. This value must be between 1 and 500.

Restrictions

Only Administrators and Operators can issue this command.

Example

To config the Switch’s MAC address table notification global settings:

```
DWS-3160-24PC:admin# config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DWS-3160-24PC:admin#
```

41-4 config mac_notification ports

Description

This command is used to configure the port’s MAC address table notification status settings.

Format

config mac_notification ports [<portlist> | all] [enable | disable]

Parameters

<portlist> - Enter a list of ports used for the configuration here. **all** - Specifies that all the ports will be used for this configuration.
enable - Enable the port’s MAC address table notification. **disable** - Disable the port’s MAC address table notification.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable 7th port’s MAC address table notification:

```
DWS-3160-24PC:admin# config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DWS-3160-24PC:admin#
```

41-5 show mac_notification

Description

This command is used to display the Switch’s MAC address table notification global settings.

Format

show mac_notification

Parameters

None.

Restrictions

None.

Example

To display the Switch’s MAC address table notification global settings:

```
DWS-3160-24PC:admin#show mac_notification
Command: show mac_notification

Global MAC Notification Settings

State        : Enabled
Interval     : 1
History Size : 500

DWS-3160-24PC:admin#
```

41-6 show mac_notification ports

Description

This command is used to display the port’s MAC address table notification status settings.

Format

show mac_notification ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a list of ports used for the configuration here.

Restrictions

None.

Example

To display all port’s MAC address table notification status settings:

```
DWS-3160-24PC:admin#show mac_notification ports
Command: show mac_notification ports

Port #  MAC Address Table Notification State
------  ------------------------------------
1                    Disabled
2                    Disabled
3                    Disabled
4                    Disabled
5                    Disabled
6                    Disabled
7                    Enabled
8                    Disabled
9                    Disabled
10                   Disabled
11                   Disabled
12                   Disabled
13                   Disabled
14                   Disabled
15                   Disabled
16                   Disabled
17                   Disabled
18                   Disabled
19                   Disabled
20                   Disabled
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Chapter 42 MAC-based Access Control Command List

enable mac_based_access_control

disable mac_based_access_control

config mac_based_access_control password <passwd 16>

config mac_based_access_control method [local | radius]

config mac_based_access_control guest_vlan ports <portlist>

config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | mode [port_based | host_based] | aging_time [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1-1000> | no_limit]}(1)

create mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]

delete mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]

clear mac_based_access_control auth_state [ports [all | <portlist>] | mac_addr <macaddr>]

create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> | vlanid < vlanid 1-4094>]}

config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]

delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

config mac_based_access_control authorization attributes {radius [enable | disable] | local [enable | disable]}(1)

show mac_based_access_control {ports {<portlist>}}

show mac_based_access_control_local {[mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

show mac_based_access_control auth_state ports {<portlist>}

config mac_based_access_control max_users [<value 1-1000> | no_limit]

config mac_based_access_control trap state [enable | disable]

config mac_based_access_control log state [enable | disable]

42-1 enable mac_based_access_control

Description

This command is used to enable MAC-based Access Control.

Format

enable mac_based_access_control

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the MAC-based Access Control global state:

```
DWS-3160-24PC:admin# enable mac_based_access_control
Command: enable mac_based_access_control

Success.

DWS-3160-24PC:admin#
```

42-2 disable mac_based_access_control

Description

This command is used to disable MAC-based Access Control.

Format

disable mac_based_access_control

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the MAC-based Access Control global state:

```
DWS-3160-24PC:admin# disable mac_based_access_control
Command: disable mac_based_access_control

Success.

DWS-3160-24PC:admin#
```

42-3 config mac_based_access_control password

Description

This command is used to configure the RADIUS authentication password for MAC-based Access Control.

Format

config mac_based_access_control password <passwd 16>

Parameters

password - In RADIUS mode, the Switch will communicate with the RADIUS server using this password. The maximum length of the key is 16.

<password> - Enter the password used here. The default password is “default”.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the MAC-based Access Control password:

```
DWS-3160-24PC:admin# config mac_based_access_control password switch
Command: config mac_based_access_control password switch

Success.

DWS-3160-24PC:admin#
```

42-4 config mac_based_access_control method

Description

This command is used to configure the MAC-based Access Control authentication method.

Format

config mac_based_access_control method [local | radius]

Parameters

local - Specifies to authenticate via the local database.

radius - Specifies to authenticate via a RADIUS server.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the MAC-based Access Control authentication method as local:

```
DWS-3160-24PC:admin# config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

DWS-3160-24PC:admin#
```

42-5 config mac_based_access_control guest_vlan

Description

This command is used to assign a specific port list to the MAC-based Access Control guest VLAN. Ports that are not contained in port list will be removed from the MAC-based Access Control guest VLAN.

Format

config mac_based_access_control guest_vlan ports <portlist>

Parameters

ports - Specifies MAC-based Access Control guest VLAN membership.
<portlist> - Enter the list of port used for this configuration here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the MAC-based Access Control guest VLAN membership:

```
DWS-3160-24PC:admin#config mac_based_access_control guest_vlan ports 11
Command: config mac_based_access_control guest_vlan ports 11

Success.

DWS-3160-24PC:admin#
```

42-6 config mac_based_access_control ports

Description

This command is used to configure the MAC-based Access Control port’s setting.

When the MAC-based Access Control function is enabled for a port and the port is not a MAC-based Access Control guest VLAN member, the user who is attached to this port will not be forwarded unless the user passes the authentication.

- A user that does not pass the authentication will not be serviced by the Switch.
- If the user passes the authentication, the user will be able to forward traffic operated under the assigned VLAN.

When the MAC-based Access Control function is enabled for a port, and the port is a MAC-based Access Control guest VLAN member, the port(s) will be removed from the original VLAN(s) member ports, and added to MAC-based Access Control guest VLAN member ports.

- Before the authentication process starts, the user is able to forward traffic under the guest VLAN.
- After the authentication process, the user will be able to access the assigned VLAN.

If the port authorize mode is port based mode, when the port has been moved to the authorized VLAN, the subsequent users will not be authenticated again. They will operate in the current authorized VLAN.

If the port authorize mode is host based mode, then each user will be authorized individually and be capable of getting its own assigned VLAN.

If port’s block time is set to” infinite”, it means that a failed authentication client will never be blocked. Block time will be set to “0”.

Format

config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | mode [port_based | host_based] | aging_time [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1-1000> | no_limit]}(1)

Parameters

ports - Specifies a range of ports for configuring the MAC-based Access Control function parameters.
- **<portlist>** - Enter the list of port used for this configuration here.
- **all** - Specifies all existed ports of Switch for configuring the MAC-based Access Control function parameters.

state - (Optional) Specifies whether the port’s MAC-based Access Control function is enabled or disabled.
- **enable** - Specifies that the port's MAC-based Access Control states will be enabled.
- **disable** - Specifies that the port's MAC-based Access Control states will be disabled.

mode - (Optional) Specifies the MAC-based access control port mode used.
- **port_based** - Specifies that the MAC-based access control port mode will be set to port-based.
- **host_based** - Specifies that the MAC-based access control port mode will be set to host-based.

aging_time - (Optional) A time period during which an authenticated host will be kept in an authenticated state. When the aging time has timed-out, the host will be moved back to unauthenticated state.
- **infinite** - If the aging time is set to infinite, it means that authorized clients will not be aged out automatically.
- **<min 1-1440>** - Enter the aging time value here. This value must be between 1 and 1440 minutes.

block_time - (Optional) If a host fails to pass the authentication, the next authentication will not start within the block time unless the user clears the entry state manually. If the block time is set to 0, it means do not block the client that failed authentication.
- **<sec 0-300>** -Enter the block time value here. This value must be between 0 and 300 seconds.

max_users - (Optional) Specifies maximum number of users per port.
- **<value 1-1000>** - Enter the maximum number of users per port here. This value must be between 1 and 1000.
- **no_limit** - Specifies to not limit the maximum number of users on the port. The default value is 128.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure an unlimited number of maximum users for MAC-based Access Control on ports 1 to 8:

```
DWS-3160-24PC:admin# config mac_based_access_control ports 1-8 max_users
no_limit
Command: config mac_based_access_control ports 1-8 max_users no_limit

Success.

DWS-3160-24PC:admin#
```

To configure the MAC-based Access Control timer parameters to have an infinite aging time and a block time of 120 seconds on ports 1 to 8:

```
DWS-3160-24PC:admin# config mac_based_access_control ports 1-8 aging_time
infinite block_time 120
Command: config mac_based_access_control ports 1-8 aging_time infinite
block_time 120

Success.

DWS-3160-24PC:admin#
```

42-7 create mac_based_access_control

Description

This command is used to assign a static 802.1Q VLAN as a MAC-based Access Control guest VLAN.

Format

create mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]

Parameters

guest_vlan - Specifies MAC-based Access Control guest VLAN by name, it must be a static 1Q VLAN. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
guest_vlanid - Specifies MAC-based Access Control guest VLAN by VID, it must be a static 1Q VLAN. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a MAC-based Access Control guest VLAN:

```
DWS-3160-24PC:admin#create mac_based_access_control guest_vlan mbacv15
Command: create mac_based_access_control guest_vlan mbacv15

Success.

DWS-3160-24PC:admin#
```

42-8 delete mac_based_access_control

Description

This command is used to remove a MAC-based Access Control guest VLAN.

Format

delete mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]

Parameters

guest_vlan - Specifies the name of the MAC-based Access Control's guest VLAN. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
guest_vlanid - Specifies the VID of the MAC-based Access Control's guest VLAN. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the MAC-based Access Control guest VLAN called 'mbacv15':

```
DWS-3160-24PC:admin# delete mac_based_access_control guest_vlan mbacv15
Command: delete mac_based_access_control guest_vlan mbacv15

Success.

DWS-3160-24PC:admin#
```

42-9 clear mac_based_access_control auth_state

Description

This command is used to clear the authentication state of a user (or port). The port (or the user) will return to an un-authenticated state. All the timers associated with the port (or the user) will be reset.

Format

clear mac_based_access_control auth_state [ports [all | <portlist>] | mac_addr <macaddr>]

Parameters

ports - Specifies the port range to delete MAC addresses on them.
all - Specifies that all MAC-based Access Control enabled ports to delete MAC addresses.
<portlist> - Enter the list of port used for this configuration here.

mac_addr - To delete a specified host with this MAC address.
<macaddr> - Enter the MAC address used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear MAC-based Access Control clients' authentication information for all ports:

```
DWS-3160-24PC:admin# clear mac_based_access_control auth_state ports all
Command: clear mac_based_access_control auth_state ports all

Success.

DWS-3160-24PC:admin#
```

To delete the MAC-based Access Control authentication information for the host that has a MAC address of 00-00-00-47-04-65:

```
DWS-3160-24PC:admin# clear mac_based_access_control auth_state mac_addr 00-00-
00-47-04-65
Command: clear mac_based_access_control auth_state mac_addr 00-00-00-47-04-65

Success.

DWS-3160-24PC:admin#
```

42-10 create mac_based_access_control_local

Description

This command is used to create a MAC-based Access Control local database entry that will be used for authentication. This command can also Specifies the VLAN that an authorized host will be assigned to.

Format

create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> | vlanid < vlanid 1-4094>]}

Parameters

mac - Specifies the MAC address that can pass local authentication.
<macaddr> - Enter the MAC address used here.

vlan - (Optional) Specifies the target VLAN by using the VLAN name. When this host is authorized, it will be assigned to this VLAN.
<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

vlanid - (Optional) Specifies the target VLAN by using the VID. When this host is authorized, it will be assigned to this VLAN if the target VLAN exists.
<vlanid 1-4094> - Enter the VLAN ID here. This value must be between 1 and 4094.

If no vlanid or vlan parameter is specified, not Specifies the target VLAN for this host.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create one MAC-based Access Control local database entry for MAC address 00-00-00-00-00-01 and Specifies that the host will be assigned to the "default" VLAN after the host has been authorized:

```
DWS-3160-24PC:admin# create mac_based_access_control_local mac 00-00-00-00-00-
01 vlan default
Command: create mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default

Success.

DWS-3160-24PC:admin#
```

42-11 config mac_based_access_control_local

Description

This command is used to configure a MAC-based Access Control local database entry.

Format

config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]

Parameters

mac - Specifies the authenticated host's MAC address.
<macaddr> - Enter the MAC address used here.

vlan - Specifies the target VLAN by VLAN name. When this host is authorized, the host will be assigned to this VLAN.
<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

vlanid - Specifies the target VLAN by VID. When this host is authorized, the host will be assigned to this VLAN if the target VLAN exists.
<vlanid 1-4094> - Enter the VLAN ID here. This value must be between 1 and 4094.

clear_vlan - Not Specifies the target VLAN. When this host is authorized, will not assign target VLAN.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the target VLAN "default" for the MAC-based Access Control local database entry 00-00-00-00-00-01:

```
DWS-3160-24PC:admin# config mac_based_access_control_local mac 00-00-00-00-00-
01 vlan default
Command: config mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default

Success.

DWS-3160-24PC:admin#
```

42-12 delete mac_based_access_control_local

Description

This command is used to delete a MAC-based Access Control local database entry.

Format

delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

mac - Delete local database entry by specific MAC address. **<macaddr>** - Enter the MAC address used here.
vlan - Delete local database entries by specific target VLAN name. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Delete local database entries by specific target VLAN ID. **<vlanid 1-4094> -** Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the MAC-based Access Control local database entry for MAC address 00-00-00-00-00-01:

```
DWS-3160-24PC:admin# delete mac_based_access_control_local mac 00-00-00-00-00-
01
Command: delete mac_based_access_control_local mac 00-00-00-00-00-01

Success.

DWS-3160-24PC:admin#
```

To delete the MAC-based Access Control local database entry for the VLAN name VLAN3:

```
DWS-3160-24PC:admin# delete mac_based_access_control_local vlan VLAN3
Command: delete mac_based_access_control_local vlan VLAN3

Success.

DWS-3160-24PC:admin#
```

42-13 config mac_based_access_control authorization attributes

Description

This command is used to enable or disable the acceptation of an authorized configuration.

When authorization is enabled for MAC-based Access Controls with RADIUS authentication, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted if the global authorization status is enabled.

When authorization is enabled for MAC-based Access Controls with local authentication, the authorized attributes assigned by the local database will be accepted.

Format

config mac_based_access_control authorization attributes {radius [enable | disable] | local [enable | disable]}(1)

Parameters

radius - (Optional) If specified to enable, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted if the global authorization status is enabled. The default state is enabled.
enable - Specifies that the RADIUS attributes will be enabled.
disable - Specifies that the RADIUS attributes will be disabled.

local - (Optional) If specified to enable, the authorized attributes assigned by the local database will be accepted if the global authorization status is enabled. The default state is enabled.
enable - Specifies that the local attributes will be enabled.
disable - Specifies that the local attributes will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

The following example will disable the configuration authorized from the local database:

```
DWS-3160-24PC:admin# config mac_based_access_control authorization attributes
local disable
Command: config mac_based_access_control authorization attributes local disable

Success.

DWS-3160-24PC:admin#
```

42-14 show mac_based_access_control

Description

This command is used to display the MAC-based Access Control setting.

Format

show mac_based_access_control {ports {<portlist>}}

Parameters

ports – (Optional) Displays the MAC-based Access Control settings for a specific port or range of ports. **<portlist>** - (Optional) Enter the list of port used for this configuration here.
If no parameter is specified, the global MAC-based Access Control settings will be displayed.

Restrictions

None.

Example

To display the MAC-based Access Control port configuration for ports 5 to 10:

```
DWS-3160-24PC:admin#show mac_based_access_control ports 5-10
Command: show mac_based_access_control ports 5-10

Port    State     Aging Time   Block Time  Auth Mode    Max User
                    (min)        (sec)
-----  --------   ----------   ---------   ----------   --------
5      Disabled   Infinite     120         Host-based   No Limit
6      Disabled   Infinite     120         Host-based   No Limit
7      Disabled   Infinite     120         Host-based   No Limit
8      Disabled   Infinite     120         Host-based   No Limit
9      Disabled   1440         300         Host-based   128
10     Disabled   1440         300         Host-based   128

DWS-3160-24PC:admin#
```

42-15 show mac_based_access_control_local

Description

This command is used to display the MAC-based Access Control local database entry(s).

Format

show mac_based_access_control_local {[mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

mac - (Optional) Displays MAC-based Access Control local database entries for a specific MAC address.
<macaddr> - Enter the MAC address used here.

vlan - (Optional) Displays MAC-based Access Control local database entries for a specific target VLAN name.
<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

vlanid - (Optional) Displays MAC-based Access Control local database entries for a specific target VLAN ID.
<vlanid 1-4094> - Enter the VLAN ID here. This value must be between 1 and 4094.

If the parameter is no specified, displays all MAC-based Access Control local database entries.

Restrictions

None.

Example

To display MAC-based Access Control local database for the VLAN called ‘default’:

```
DWS-3160-24PC:admin#show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default

MAC Address        VID
-----------------  ----
00-00-00-00-00-01  1

Total Entries:1

DWS-3160-24PC:admin#
```

42-16 show mac_based_access_control auth_state

Description

This command is used to display the MAC-based Access Control authentication status.

Format

show mac_based_access_control auth_state ports {<portlist>}

Parameters

ports - Display authentication status by specific port.
<portlist> - (Optional) Enter the list of port used for this configuration here.

If not specified port(s), it will display all of MAC-based Access Control ports authentication status.

Restrictions

None.

Example

To display the MAC-based Access Control authentication status on port 1-4

```
DWS-3160-24PC:admin#show mac_based_access_control auth_state ports 1-4
Command: show mac_based_access_control auth_state ports 1-4

 (P): Port-based

Port MAC Address          State          VID  Priority Aging Time/
                                                       Block Time
---- -------------------- -------------- ---- -------- ------------
2    00-22-B0-3C-DD-C0    Blocked        -    -        101

Total Authenticating Hosts  : 0
Total Authenticated Hosts   : 0
Total Blocked Hosts         : 1

DWS-3160-24PC:admin#
```

42-17 config mac_based_access_control max_users

Description

This command is used to configure the maximum number of authorized clients.

Format

config mac_based_access_control max_users [<value 1-1000> | no_limit]

Parameters

max_users - Specifies to set the maximum number of authorized clients on the whole device.
- **<value 1-1000>** - Enter the maximum users here. This value must be between 1 and 1000.
- **no_limit** - Specifies to not limit the maximum number of users on the system. By default, there is no limit on the number of users.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the maximum number of users of the MAC-based Access Control system supports to 128:

```
DWS-3160-24PC:admin# config mac_based_access_control max_users 128
Command: config mac_based_access_control max_users 128

Success.

DWS-3160-24PC:admin#
```

42-18 config mac_based_access_control trap state

Description

This command is used to enable or disable sending of MAC-based Access Control traps.

Format

config mac_based_access_control trap state [enable | disable]

Parameters

enable - Enable trap for MAC-based Access Control. The trap of MAC-based Access Control will be sent out.

disable - Disable trap for MAC-based Access Control.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable trap state of MAC-based Access Control:

```
DWS-3160-24PC:admin# config mac_based_access_control trap state enable
Command: config mac_based_access_control trap state enable

Success.

DWS-3160-24PC:admin#
```

42-19 config mac_based_access_control log state

Description

This command is used to enable or disable generating of MAC-based Access Control logs.

Format

config mac_based_access_control log state [enable | disable]

Parameters

enable - Enable log for MAC-based Access Control. The log of MAC-based Access Control will be generated.

disable - Disable log for MAC-based Access Control.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable log state of MAC-based Access Control:

```
DWS-3160-24PC:admin# config mac_based_access_control log state disable
Command: config mac_based_access_control log state disable

Success.

DWS-3160-24PC:admin#
```

Chapter 43 MAC-based VLAN Command List

create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
show mac_based_vlan {mac_address <macaddr> | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

43-1 create mac_based_vlan

Description

This command is used to create a static MAC-based VLAN entry. There is a global limitation of the maximum entries supported for the static MAC-based entry.

Format

create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

mac_address - Specifies the MAC address used. **<macaddr>** - Enter the MAC address here.
vlan - The VLAN to be associated with the MAC address. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specifies the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a static MAC-based VLAN entry:

```
DWS-3160-24PC:admin# create mac_based_vlan mac_address 00-11-22-33-44-55 vlanid
100
Command: create mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100


Success.


DWS-3160-24PC:admin#
```

43-2 delete mac_based_vlan

Description

This command is used to delete a static MAC-based VLAN entry.

Format

delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

mac_address - (Optional) Specifies the MAC address used.
<macaddr> - Enter the MAC address used here.

vlan - (Optional) The VLAN to be associated with the MAC address.
<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

vlanid - (Optional) Specifies the VLAN by VLAN ID.
<vlanid 1-4094> - Enter the VLAN ID here. This value must be between 1 and 4094.

If no parameter is specified, ALL static configured entries will be removed.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a static MAC-based VLAN entry:

```
DWS-3160-24PC:admin# delete mac_based_vlan mac_address 00-11-22-33-44-55 vlanid
100
Command: delete mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100


Success.


DWS-3160-24PC:admin#
```

43-3 show mac_based_vlan

Description

This command is used to display static or dynamic MAC-based VLAN entry. If the MAC address and VLAN is not specified, all static and dynamic entries will be displayed.

Format

show mac_based_vlan {mac_address <macaddr> | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

mac_address - (Optional) Specifies the entry that you would like to display.
<macaddr> - Enter the MAC address used here.

vlan - (Optional) Specifies the VLAN that you would like to display.
    <vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

vlanid - (Optional) Specifies the VLAN by VLAN ID.
    <vlanid 1-4094> - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

None.

Example

In the following example, MAC address “00-80-c2-33-c3-45” is assigned to VLAN 300 by manual config. It is assigned to VLAN 400 by Voice VLAN. Since Voice VLAN has higher priority than manual configuration, the manual configured entry will become inactive. To display the MAC-based VLAN entry:

```
DWS-3160-24PC:admin#show mac_based_vlan
Command: show mac_based_vlan

    MAC Address       VLAN ID        Status        Type
-----------------     -------        --------      -------------------
00-80-e0-14-a7-57     200            Active        Static
00-80-c2-33-c3-45     300            Inactive      Static
00-80-c2-33-c3-45     400            Active        Voice VLAN

Total Entries : 3

DWS-3160-24PC:admin#
```

Chapter 44 Mirror Command List

config mirror port <port> {[add | delete] source ports <portlist> [rx | tx | both]}
enable mirror
disable mirror
show mirror

44-1 config mirror

Description

This command is used to configure a mirror port on the Switch. Traffic from any source port to a target port can be mirrored for real-time analysis. A logic analyzer or an RMON probe then can be attached to study the traffic crossing the source port in a completely unobtrusive manner.

NOTE: The target port must be configured in the same VLAN and operates at the same speed as the source port. If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that of the target port.

Format

config mirror port <port> {[add | delete] source ports <portlist> [rx | tx | both]}

Parameters

port - The port that will receive the packets duplicated at the mirror port.
 <port> - Enter the port number to be configured here.

add - (Optional) The mirror entry to be added.
delete - (Optional) The mirror entry to be deleted.

source ports - (Optional) The port that will be mirrored. All packets entering and leaving the source port can be duplicated in the mirror port.
 <portlist> - Enter the list of port to be configured here.

rx - (Optional) Allows the mirroring packets received (flowing into) the port or ports in the port list.

tx - (Optional) Allows the mirroring packets sent (flowing out of) the port or ports in the port list.

both - (Optional) Mirrors all the packets received or sent by the port or ports in the port list.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add the mirroring ports:

```
DWS-3160-24PC:admin# config mirror port 3 add source ports 7-12 both
Command: config mirror port 5 add source ports 1-5 both

Success.

DWS-3160-24PC:admin#
```

44-2 enable mirror

Description

This command is used to enable the mirror function without having to modify the mirror session configuration.

Format

enable mirror

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable mirroring function:

```
DWS-3160-24PC:admin# enable mirror
Command: enable mirror

Success.

DWS-3160-24PC:admin#
```

44-3 disable mirror

Description

This command is used to disable the mirror function without having to modify the mirror session configuration.

Format

disable mirror

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable mirroring function:

```
DWS-3160-24PC:admin# disable mirror
Command: disable mirror

Success.

DWS-3160-24PC:admin#
```

44-4 show mirror

Description

This command is used to display the mirror function’s state and mirror session configuration on the Switch.

Format

show mirror

Parameters

None.

Restrictions

None.

Example

To display mirroring configuration:

```
DWS-3160-24PC:admin#show mirror
Command: show mirror

Current Settings
Mirror Status: Enabled
Target Port  : 3
Mirrored Port
           RX: 7-12
           TX: 7-12

DWS-3160-24PC:admin#
```

Chapter 45 MLD Snooping Command List

config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_done [enable | disable] | report_suppression [enable | disable]}(1)

config mld_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version <value 1-2>}(1)

config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

enable mld_snooping

disable mld_snooping

show mld_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

show mld_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipv6addr>}} {data_driven}

show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}

create mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

delete mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

config mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr> [add | delete] <portlist>

show mld_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>}

config mld_snooping data_driven_learning [all | vlan_name <vlan_name> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}

config mld_snooping data_driven_learning max_learned_entry <value 1-1024>

clear mld_snooping data_driven_group [all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipv6addr> | all]]

show mld_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist>]

clear mld_snooping statistics counter

config mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]

show mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]

45-1 config mld_snooping

Description

This command is used to configure MLD snooping on the Switch.

Format

config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_done [enable | disable] | report_suppression [enable | disable]}(1)

Parameters

vlan_name - Specifies the name of the VLAN for which MLD snooping is to be configured.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters

long.

vlanid - Specifies the ID of the VLAN for which MLD snooping is to be configured.
<vlanid_list> - Enter the VLAN ID list here.

all - Specifies all VLANs for which MLD snooping is to be configured.

state - (Optional) Enable or disable MLD snooping for the chosen VLAN.
enable - Enter enable here to enable MLD snooping for the chosen VLAN.
disable - Enter disable here to disable MLD snooping for the chosen VLAN.

fast_done - (Optional) Enable or disable MLD snooping fast_leave function.
enable - Enter enable here to enable MLD snooping fast_leave function. If enable, the membership is immediately removed when the system receive the MLD leave message.
disable - Enter disable here to disable MLD snooping fast_leave function.

report_suppression - (Optional) When MLD report suppression is enabled (the default), the Switch sends the first MLD report from all hosts for a group to all the multicast routers. The Switch does not send the remaining MLD reports for the group to the multicast routers. If the multicast router query includes requests only for MLDv1 reports, the Switch forwards only the first MLDv1 report from all hosts for a group to all the multicast routers. If the multicast router query also includes requests for MLDv2 reports, the Switch forwards all MLDv2 reports for a group to the multicast devices.
enable - Enter enable to enable the report suppression.
disable - Enter disable to disable the report suppression.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure MLD snooping:

```
DWS-3160-24PC:admin#config mld_snooping vlan_name v2 state enable
Command: config mld_snooping vlan_name v2 state enable

Success.

DWS-3160-24PC:admin#
```

45-2 config mld_snooping querier

Description

This command is used to configure the timer in seconds between general query transmissions, the maximum time in seconds to wait for reports from listeners, and the permitted packet loss that is guaranteed by MLD snooping.

Format

config mld_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version <value 1-2>}(1)

Parameters

vlan_name - Specifies the name of the VLAN for which MLD snooping querier is to be

configured.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN for which MLD snooping querier is to be configured.
<vlanid_list> - Enter the VLAN ID list here.
all - Specifies all VLANs for which MLD snooping querier is to be configured.

query_interval - (Optional) Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.
<sec 1-65535> - Enter the query interval value here. This value must be between 1 and 65535 seconds.

max_reponse_time - (Optional) Specifies the maximum time in seconds to wait for reports from listeners. The default setting is 10 seconds.
<sec 1-25> - Enter the maximum response time value here. This value must be between 1 and 25 seconds.

robustness_variable - (Optional) Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following MLD message intervals:
<value 1-7> - Enter the robustness variable value here. This value must be between 1 and 7.

1. Group listener interval—Amount of time that must pass before a multicast router decides there are no more listeners of a group on a network. This interval is calculated as follows: (robustness variable * query interval) + (1 * query response interval).
2. Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable * query interval) + (0.5 * query response interval).
3. Last listener query count—Number of group-specific queries sent before the router assumes there are no local listeners of a group. The default number is the value of the robustness variable.
4. By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be loosely.

last_listener_query_interval - (Optional) Specifies the maximum amount of time between group-specific query messages, including those sent in response to done-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last listener of a group.
<sec 1-25> - Enter the last listener query interval value here. This value must be between 1 and 25 seconds.

state - (Optional) This allows the Switch to be specified as an MLD Querier (sends MLD query packets) or a Non-Querier (does not send MLD query packets). Set to enable or disable.
enable - Enter enable to enable the MLD querier state here.
disable - Enter disable to disable the MLD querier state here.

version - (Optional) Specifies the version of MLD packet that will be sent by this port. If a MLD packet received by the interface has a version higher than the specified version, this packet will be dropped.
<value 1-2> - Enter the version number value here. This value must be between 1 and 2.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the MLD snooping querier:

```
DWS-3160-24PC:admin#config mld_snooping querier all query_interval 125 state
enable
Command: config mld_snooping querier all query_interval 125 state enable

Success.

DWS-3160-24PC:admin#
```

45-3 config mld_snooping router_ports

Description

This command is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router, regardless of protocol.

Format

config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Parameters

vlan - Specifies the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long. **vlanid** - Specifies the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
add - Specifies to add the router ports. **delete** - Specifies to delete the router ports.
<portlist> - Specifies a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set up static router ports:

```
DWS-3160-24PC:admin#config mld_snooping mrouter_ports vlanid 2 add 1-10
Command: config mld_snooping mrouter_ports vlanid 2 add 1-10

Success.

DWS-3160-24PC:admin#
```

45-4 config mld_snooping router_ports_forbidden

Description

This command is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.

Format

config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Parameters

vlan - Specifies the name of the VLAN on which the router port resides.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the router port resides.
<vlanid_list> - Enter the VLAN ID list here.

add - Specifies to add the router ports.
delete - Specifies to delete the router ports.

<portlist> - Specifies a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set up port range 11-12 to forbidden router ports of VLAN ID 2:

```
DWS-3160-24PC:admin#config mld_snooping mrouter_ports_forbidden vlanid 2 add
11-12
Command: config mld_snooping mrouter_ports_forbidden vlanid 2 add 11-12

Success.

DWS-3160-24PC:admin#
```

45-5 enable mld_snooping

Description

This command is used to enable MLD snooping on the Switch. The forward MC router only function is disabled by default. If forward multicast router only is enabled, the Switch will forward all multicast traffic to the multicast router, only. Otherwise, the Switch forwards all multicast traffic to any IP router.

Format

enable mld_snooping

Parameters

When the Switch receives an MLD report packet from a port, this port will be learned as a member port of the multicast group that the port is reported, and the router will be a default member of this multicast group. The multicast packet destined for this multicast group will be forwarded to all the members of this multicast group.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable MLD snooping on the Switch:

```
DWS-3160-24PC:admin# enable mld_snooping
Command: enable mld_snooping

Success.

DWS-3160-24PC:admin#
```

45-6 disable mld_snooping

Description

This command is used to disable MLD snooping on the Switch.

Format

disable mld_snooping

Parameters

When the Switch receives an MLD report packet from a port, this port will be learned as a member port of the multicast group that the port is reported, and the router will be a default member of this multicast group. The multicast packet destined for this multicast group will be forwarded to all the members of this multicast group.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable MLD snooping on the Switch:

```
DWS-3160-24PC:admin# disable mld_snooping
Command: disable mld_snooping

Success.

DWS-3160-24PC:admin#
```

45-7 show mld_snooping

Description

This command is used to display the current MLD snooping configuration on the Switch.

Format

show mld_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view the MLD snooping configuration.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - (Optional) Specifies the ID of the VLAN for which you want to view the MLD snooping configuration.
<vlanid_list> - Enter the VLAN ID list here.

If VLAN is not specified, the system will display all current MLD snooping configurations.

Restrictions

None.

Example

To display MLD snooping:

```
DWS-3160-24PC:admin#show mld_snooping
Command: show mld_snooping

 MLD Snooping Global State              : Enabled
 Data Driven Learning Max Entries       : 128

 VLAN Name                       : default
 Query Interval                  : 125
 Max Response Time               : 10
 Robustness Value                : 2
 Last Listener Query Interval    : 1
 Querier State                   : Enabled
 Querier Role                    : Non-Querier
 Querier IP                      : ::
 Querier Expiry Time             : 0 secs
 State                           : Disabled
 Fast Done                       : Disabled
 Rate Limit                      : No Limitation
 Report Suppression              : Enabled
 Version                         : 2
 Data Driven Learning State      : Enabled
 Data Driven Learning Aged Out   : Disabled
 Data Driven Group Expiry Time   : 260

 VLAN Name                       : v2
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

45-8 show mld_snooping group

Description

This command is used to display the current MLD snooping group information on the Switch.

Format

show mld_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipv6addr>}} {data_driven}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view MLD snooping group information. If VLAN and ports and IP address are not specified, the system will display all current MLD snooping group information.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - (Optional) Specifies the ID of the VLAN for which you want to view MLD snooping group information.
<vlanid_list> - Enter the VLAN ID list here.

ports - (Optional) Specifies a list of ports for which you want to view MLD snooping group information.
<portlist> - Enter the list of port here.

<ipv6addr> - (Optional) Specifies the group IPv6 address for which you want to view MLD snooping group information.

data_driven - (Optional) Display the data driven groups.

Restrictions

None.

Example

To display an MLD snooping group when MLD v2 is supported:

The first item means that for ports 1-2, the data from the 2001::1/FE1E::1 will be forwarded.

The second item means that for port 3, the data from the 2002::2/FE1E::1 must not be forwarded.

The third item means that for ports 4-5, the data from FE1E::2 will be forwarded, MLD v1 group doesn't care about the source address.

The fourth item is a data-driven learned entry. The member port list is empty. The multicast packets will be forwarded to the router ports. If the router port list is empty, the packet will be dropped.

```
DWS-3160-24PC:admin# show mld_snooping group
Command: show mld_snooping group

Source/Group        : 2001::1/FE1E::1
VLAN Name/VID       : default/1
Member Ports        : 1-2
UP Time             : 26
Expiry Time         : 258
Filter Mode         : INCLUDE

Source/Group        : 2002::2/FE1E::1
VLAN Name/VID:      : default/1
Member Ports        : 3
UP Time             : 29
Expiry Time         : 247
Filter Mode         : EXCLUDE

Source/Group        : NULL/FE1E::2
VLAN Name/VID       : default/1
Member Ports        : 4-5
UP Time             : 40
Expiry Time         : 205
Filter Mode         : EXCLUDE

Source/Group        : NULL/FF1E::5
VLAN Name/VID       : default/1
Reports             : 0
Member Ports        :
Router Ports        : 24
UP Time             : 100
Expiry Time         : 200
Filter Mode         : EXCLUDE

Total Entries : 4

DWS-3160-24PC:admin#
```

```
DWS-3160-24PC:admin# show mld_snooping group data_driven
Command: show mld_snooping group data_driven

Source/Group        : NULL/FF1E::5
VLAN Name/VID       : default/1
Member Ports        :
Router Ports        : 24
UP Time             : 100
Expiry Time         : 200
Filter Mode         : EXCLUDE

Total Entries : 1

DWS-3160-24PC:admin#
```

45-9 show mld_snooping forwarding

Description

This command is used to display the Switch's current MLD snooping forwarding table. It provides an easy way for users to check the list of ports that the multicast group that comes from specific sources will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding VLAN. The MLD snooping further restricts the forwarding ports.

Format

show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view MLD snooping forwarding table information.

<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - (Optional) Specifies the ID of the VLAN for which you want to view MLD snooping forwarding table information.

<vlanid_list> - Enter the VLAN ID list here.

If no parameter is specified, the system will display all current MLD snooping forwarding table entries of the Switch.

Restrictions

None.

Example

To display all MLD snooping forwarding entries located on the Switch.

```
DWS-3160-24PC:admin# show mld_snooping forwarding
Command: show mld_snooping forwarding

VLAN Name      : default
Source IP      : 2001::1
Multicast Group: FE1E::1
Port Member    : 2,7

VLAN Name      : default
Source IP      : 2001::2
Multicast Group: FF1E::1
Port Member    : 5

Total Entries : 2

DWS-3160-24PC:admin#
```

45-10 show mld_snooping mrouter_ports

Description

This command is used to display the configured router ports on the Switch.

Format

show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}

Parameters

vlan - Specifies the name of the VLAN on which the router port resides.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the router port resides.
<vlanid_list> - Enter the VLAN ID list here.
all - Specifies all VLANs on which the router port resides.

static - (Optional) Displays router ports that have been statically configured.

dynamic - (Optional) Displays router ports that have been dynamically configured.

forbidden - (Optional) Displays forbidden router ports that have been statically configured.

If no parameter is specified, the system will display all currently configured router ports on the Switch.

Restrictions

None.

Example

To display the mld_snooping router ports:

```
DWS-3160-24PC:admin# show mld_snooping router_ports
Command: show mld_snooping router_ports

VLAN Name                : default
Static Router Port       :
Dynamic Router Port      : 1-10
          Router IP      : FE08::1
Forbidden router port    :

Total Entries : 1

DWS-3160-24PC:admin#
```

45-11 create mld_snooping static_group

Description

This command is used to create an MLD snooping static group. Member ports can be added to the static group. The static member and the dynamic member ports form the member ports of a group.

The static group will only take effect when MLD snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the MLD protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports.

For a Layer 3 device, the device is also responsible to route the packets destined for this specific group to static member ports.

The Reserved IP multicast addresses FF0x::/16 must be excluded from the configured group.

The VLAN must be created first before a static group can be created.

Format

create mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

Parameters

vlan - Specifies the name of the VLAN on which the static group resides.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - Specifies the ID of the VLAN on which the static group resides.
<vlanid_list> - Enter the VLAN ID list here.

<ipv6addr> - Specifies the multicast group IPv6 address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an MLD snooping static group for VLAN ID 2, group FF1E::1:

```
DWS-3160-24PC:admin#create mld_snooping static_group vlanid 2 FF1E::1
Command: create mld_snooping static_group vlanid 2 FF1E::1

Success.

DWS-3160-24PC:admin#
```

45-12 delete mld_snooping static_group

Description

This command is used to delete an MLD Snooping multicast static group.

Format

delete mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

Parameters

vlan - Specifies the name of the VLAN on which the static group resides.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - Specifies the ID of the VLAN on which the static group resides.
<vlanid_list> - Enter the VLAN ID list here.

<ipv6addr> - Specifies the multicast group IP address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an MLD snooping static group for VLAN 1, group FF1E::1:

```
DWS-3160-24PC:admin# delete mld_snooping default FF1E::1
Command: delete mld_snooping default FF1E::1

Success.

DWS-3160-24PC:admin#
```

45-13 config mld_snooping static_group

Description

This command is used to configure an MLD snooping multicast group static member port. When a port is configured as a static member port, the MLD protocol will not operate on this port. For example, suppose that a port is a dynamic member port learned by MLD. If this port is configured as a static member later, then the MLD protocol will stop operating on this port. The MLD protocol will resume once this port is removed from static member ports.

Format

config mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr> [add | delete] <portlist>

Parameters

vlan - Specifies the name of the VLAN on which the static group resides.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - Specifies the ID of the VLAN on which the static group resides.
<vlanid_list> - Enter the VLAN ID list here.

<ipv6addr> - Specifies the multicast group IPv6 address.

add - Specifies to add the member ports.
delete - Specifies to delete the member ports.

<portlist> - Specifies a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the ports 11 and 12 from MLD snooping static member ports for group FF1E::1 on VLAN ID 2:

```
DWS-3160-24PC:admin#config mld_snooping static_group vlan v2 FF1E::1 delete 11-
12
Command: config mld_snooping static_group vlan v2 FF1E::1 delete 11-12

Success.

DWS-3160-24PC:admin#
```

45-14 show mld_snooping static_group

Description

This command used to display the MLD snooping multicast group static members.

Format

show mld_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>}

Parameters

vlan - (Optional) Specifies the name of the VLAN on which the static group resides.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - (Optional) Specifies the ID of the VLAN on which the static group resides.
<vlanid_list> - Enter the VLAN ID list here.

<ipv6addr> - (Optional) Specifies the multicast group IPv6 address.

Restrictions

None.

Example

To display all the MLD snooping static groups:

```
DWS-3160-24PC:admin#show mld_snooping static_group
Command: show mld_snooping static_group

VLAN ID/Name                     IP Address               Static Member Ports
------------------------------  ---------------------  -------------------
2   /v2                         FF1E::1                 11-12
2   /v2                         FF1E::5

 Total Entries : 2

DWS-3160-24PC:admin#
```

45-15 config mld_snooping data_driven_learning

Description

This command is used to enable or disable the data-driven learning of an MLD snooping group.

When data-driven learning is enabled for the VLAN, when the Switch receives the IP multicast traffic, on this VLAN, an MLD snooping group will be created. That is, the learning of an entry is not activated by MLD membership registration, but activated by the traffic. For an ordinary MLD snooping entry, the MLD protocol will take care the aging out of the entry. For a data-driven entry, the entry can be specified not to be aged out or to be aged out by the aged timer.

When the data driven learning is enabled, and the data driven table is not full, the multicast filtering mode for all ports is ignored. That is, the multicast packets will be forwarded to router ports. If the data driven learning table is full, the multicast packets will be forwarded according to the multicast filtering mode.

NOTE: If a data-driven group is created and MLD member ports are learned later, the entry will become an ordinary MLD snooping entry. That is, the aging out mechanism will follow the ordinary MLD snooping entry.

Format

config mld_snooping data_driven_learning [all | vlan_name <vlan_name> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)

Parameters

vlan_name - Specifies the VLAN name to be configured.
<vlan_name> - Enter the VLAN name here.
vlanid - Specifies the VLAN ID to be configured.
<vlanid_list> - Enter the VLAN ID list here.
all - Specifies that all VLANs are to be configured.

state - (Optional) Specifies to enable or disable the data driven learning of MLD snooping groups. By default, the state is enabled.
enable - Enter enable to enable the data driven learning state.
disable - Enter disable to disable the data driven learning state.

aged_out - (Optional) Enable or disable the aging out of entries. By default, the state is disabled.
enable - Enter enable to enable the aged out option.
disable - Enter disable to disable the aged out option.

expiry_time - (Optional) Specifies the data driven group lifetime, in seconds. This parameter is valid only when aged_out is enabled.
<sec 1-65535> - Enter the expiry time value here. This value must be between 1 and 65535 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the data driven learning of an MLD snooping group on the default VLAN:

```
DWS-3160-24PC:admin# config mld_snooping data_driven_learning vlan default
state enable
Command: config mld_snooping data_driven_learning vlan default state enable

Success.

DWS-3160-24PC:admin#
```

45-16 config mld_snooping data_driven_learning max_learned_entry

Description

This command is used to configure the maximum number of groups that can be learned by data driven. When the table is full, the system will stop the learning of the new data-driven groups. Traffic for the

Format

config mld_snooping data_driven_learning max_learned_entry <value 1-1024>

Parameters

max_learned_entry - Specifies the maximum number of groups that can be learned by data driven. The suggested default setting is 56. This default setting may vary depending on project.

<value 1-1024> - Enter the maximum learned entry value here. This value must be between 1 and 1024.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the maximum number of groups that can be learned by data driven:

```
DWS-3160-24PC:admin# config mld_snooping data_driven_learning max_learned_entry
50
Command: config mld_snooping data_driven_learning max_learned_entry 50

Success.

DWS-3160-24PC:admin#
```

45-17 clear mld_snooping data_driven_group

Description

This command is used to delete the MLD snooping groups learned by data driven.

Format

clear mld_snooping data_driven_group [all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipv6addr> | all]]

Parameters

all - Specifies all VLANs to which MLD snooping groups will be deleted.
vlan_name - Specifies the VLAN name.
  <vlan_name> - Enter the VLAN name here.
vlanid - Specifies the VLAN ID.
  <vlanid_list> - Enter the VLAN ID list here.

<ipaddr> - Specifies the group's IP address learned by data driven.
all - Specifies to clear all data driven groups of the specified VLAN.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete all the groups learned by data-driven:

```
DWS-3160-24PC:admin# clear mld_snooping data_driven_group all
Command: clear mld_snooping data_driven_group all

Success.

DWS-3160-24PC:admin#
```

45-18 show mld_snooping statistic counter

Description

This command is used to display the statistics counter for MLD protocol packets that are received by the Switch since MLD snooping was enabled.

Format

show mld _snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist>]

Parameters

vlan - Specifies a VLAN to be displayed.
  <vlan_name> - Enter the VLAN name here.

vlanid - Specifies a list of VLANs to be displayed.
  <vlanid_list> - Enter the VLAN ID list here.

ports - Specifies a list of ports to be displayed.
  <portlist> - Enter the list of port here.

Restrictions

None.

Example

To display MLD snooping statistics counters:

```
DWS-3160-24PC:admin#show mld_snooping statistic counter vlanid 2
Command: show mld_snooping statistic counter vlanid 2

VLAN name         : v2
--------------------------------------------------
Group Number      : 0

Receive Statistics
    Query
      MLD v1 Query                      : 0
      MLD v2 Query                      : 0
      Total                             : 0
      Dropped By Rate Limitation        : 0
      Dropped By Multicast VLAN         : 0

    Report & Done
      MLD v1 Report                     : 0
      MLD v2 Report                     : 0
      MLD v1 Done                       : 0
      Total                             : 0
      Dropped By Rate Limitation        : 0
      Dropped By Max Group Limitation   : 0
      Dropped By Group Filter           : 0
      Dropped By Multicast VLAN         : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

45-19 clear mld_snooping statistic counter

Description

This command is used to clear MLD snooping statistics counters.

Format

clear mld_snooping statistics counter

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear MLD snooping statistics counter:

```
DWS-3160-24PC:admin# clear mld_snooping statistics counter
Command: clear mld_snooping statistic counter

Success.

DWS-3160-24PC:admin#
```

45-20 config mld_snooping rate_limit

Description

This command is used to configure the rate limit of MLD control packets that are allowed by each port or VLAN.

Format

config mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]

Parameters

ports - Specifies a range of ports to be configured.
<portlist> - Enter the range of ports to be configured here.

vlanid - Specifies a range of VLANs to be configured.
<vlanid_list> - Enter the VLAN ID list here.

<value 1-1024> - Configure the rate limit of MLD control packets that the Switch can process on a specific port or VLAN. The rate is specified in packet per second. The packets that exceed the limited rate will be dropped.

no_limit - Configure the rate limit of MLD control packets that the Switch can process on a specific port or VLAN. The rate is specified in packet per second. The packets that exceed the limited rate will be dropped. The default setting is no_limit.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the MLD snooping per port rate limit:

```
DWS-3160-24PC:admin#config mld_snooping rate_limit ports 1 100
Command: config mld_snooping rate_limit ports 1 100

Success.

DWS-3160-24PC:admin#
```

45-21 show mld_snooping rate_limit

Description

This command is used to configure the rate limit of MLD control packets that are allowed by each port.

Format

show mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]

Parameters

ports - Specifies a list of ports.
<portlist> - Enter the range of ports to be configured here.

vlanid - Specifies a list of VLANs.
<vlanid_list> - Enter the VLAN ID list here.

Restrictions

None.

Example

To configure the mld_snooping per port rate_limit:

```
DWS-3160-24PC:admin#show mld_snooping rate_limit ports 1-15
Command: show mld_snooping rate_limit ports 1-15

 Port      Rate Limit
 --------  ---------------
 1         100
 2         No Limit
 3         No Limit
 4         No Limit
 5         No Limit
 6         No Limit
 7         No Limit
 8         No Limit
 9         No Limit
 10        No Limit
 11        No Limit
 12        No Limit
 13        No Limit
 14        No Limit
 15        No Limit

Total Entries: 15

DWS-3160-24PC:admin#
```

Chapter 46 MLD Snooping Multicast (MSM) VLAN Command List

create mld_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}

config mld_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ip <ipv6addr> | remap_priority [<value 0-7> | none] {replace_priority}}(1)

create mld_snooping multicast_vlan_group_profile <profile_name 1-32>

config mld_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_v6address_list>

delete mld_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]

show mld_snooping multicast_vlan_group_profile {<profile_name 1-32>}

config mld_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>

show mld_snooping multicast_vlan_group {<vlan_name 32>}

delete mld_snooping multicast_vlan <vlan_name 32>

enable mld_snooping multicast_vlan

disable mld_snooping multicast_vlan

config mld_snooping multicast_vlan forward_unmatched [disable | enable]

show mld_snooping multicast_vlan {<vlan_name 32>}

46-1 create mld_snooping multicast_vlan

Description

This command is used to create an MLD snooping multicast VLAN. More than one multicast VLANs can be created. Newly created MLD snooping multicast VLANs must use a unique VLAN ID and name. They cannot use the VLAN ID or name of any existing 802.1Q VLAN.

Also keep in mind the following conditions:

- Multicast VLANs cannot be configured or displayed using 802.1Q VLAN commands.
- An IP interface cannot be bound to a multicast VLAN.
- The multicast VLAN snooping function co-exists with the 802.1Q VLAN snooping function.

Format

create mld_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}

Parameters

<vlan_name 32> - Enter the multicast VLAN name here. This name can be up to 32 characters long.

<vlanid 2-4094> - Enter the multicast VLAN ID here. This value must be between 2 and 4094.

remap_priority - (Optional) Specifies the remap priority value, to be associated with the data traffic forwarded on the multicast VLAN.
<value 0-7> - Enter the remap priority value here. This value must be between 0 and 7.
none - Specifies that the remap priority value will be set to none. The packet’s original priority

will be used. This is the default setting.

replace_priority - (Optional) Specifies that the packet's priority will be changed by the Switch, based on the remap priority. This flag will only take effect when the remap priority is set.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an MLD snooping multicast VLAN with the VLAN name mv2 and the VID 4:

```
DWS-3160-24PC:admin#create mld_snooping multicast_vlan mv2 4
Command: create mld_snooping multicast_vlan mv2 4

Success.

DWS-3160-24PC:admin#
```

46-2 config mld_snooping multicast_vlan

Description

This command is used to add member ports and source ports to a list of multicast VLAN member ports. Member ports automatically become untagged members of the multicast VLAN and source ports automatically become tagged members of the multicast VLAN. If the port list of an existing multicast VLAN is changed without Specifiesing add or delete, the newly added port list replaces the existing port list. A member port list cannot overlap with a source port list of the same multicast VLAN. However, member ports of one multicast VLAN are allowed to overlap with member ports on a different multicast VLAN.

Format

config mld_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ip <ipv6addr> | remap_priority [<value 0-7> | none] {replace_priority}}(1)

Parameters

multicast_vlan - The name of the multicast VLAN to be configured. The maximum length is 32 characters.
<vlan_name 32> - Enter the VLAN here. The VLAN name can be up to 32 characters long.

add - (Optional) Specifies to add member ports to the multicast VLAN.
delete - (Optional) Specifies to delete member ports to the multicast VLAN.

member_port - (Optional) A member port or range of member ports to be added to the multicast VLAN. The specified range of ports will become untagged members of the multicast VLAN.
<portlist> - Enter the list of port to be configured here.

tag_member_port - (Optional) Specifies that the port or range of ports will become tagged members of the multicast VLAN.
<portlist> - Enter the list of port to be configured here.

source_port - (Optional) Specifies the port or range of ports to be added to the multicast VLAN.
<portlist> - Enter the list of port to be configured here.

untag_source_port - (Optional) Specifies the source port or range of source ports as untagged

members of the multicast VLAN. The PVID of the untagged source port is automatically changed to the multicast VLAN. Source ports must be either tagged or untagged for any single multicast VLAN, i.e. both types cannot be members of the same multicast VLAN.
<portlist> - Enter the list of port to be configured here.

state - (Optional) Used to Specifies if the multicast VLAN for a chosen VLAN should be enabled or disabled.
enable - Specifies to enable the multicast VLAN for a chosen VLAN.
disable - Specifies to disable the multicast VLAN for a chosen VLAN.

replace_source_ipv6 - (Optional) Before forwarding the report packet sent by the host, the source IP address in the join packet must be replaced by this IP address. If none is specified, the source IP address will not be replaced.
<ipv6addr> - Enter the replace source IPv6 address here.

remap_priority - (Optional) The remap priority value to be associated with the data traffic to be forwarded on the multicast VLAN. If none is specified, the packet's original priority is used. The default setting is none.
<value 0-7> - Enter the remap priority value here. This value must be between 0 and 7.

replace_priority - (Optional) The packet priority is changed to the remap_priority, but only if the remap_priority is set.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure an MLD snooping multicast VLAN with the name "mv2", make ports 1 and 3 members of the VLAN, and set the state to enable:

```
DWS-3160-24PC:admin#config mld_snooping multicast_vlan mv2 add member_port 1,3
state enable
Command: config mld_snooping multicast_vlan mv2 add member_port 1,3 state
enable


Success.


DWS-3160-24PC:admin#
```

46-3 create mld_snooping multicast_vlan_group_profile

Description

This command is used to create an MLD snooping multicast group profile on the Switch.

Format

create mld_snooping multicast_vlan_group_profile <profile_name 1-32>

Parameters

<profile_name 1-32> - Enter the multicast VLAN group profile name here. The name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an MLD snooping multicast group profile with the name “MGroup”:

```
DWS-3160-24PC:admin#create igmp_snooping multicast_vlan_group_profile MGroup
Command: create igmp_snooping multicast_vlan_group_profile MGroup

Success.

DWS-3160-24PC:admin#
```

46-4 config mld_snooping multicast_vlan_group_profile

Description

This command is used to configure an MLD snooping multicast group profile on the Switch and add or delete multicast addresses for the profile.

Format

config mld_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_v6address_list>

Parameters

multicast_vlan_group_profile - Specifies the multicast VLAN profile name. The maximum length is 32 characters.

<profile_name 1-32> - Enter the multicast VLAN group profile name here. This name can be up to 32 characters long.

add - Add a multicast address list to or from this multicast VLAN profile. The <mcast_v6address_list> can be a continuous single multicast addresses, such as FF1E::1, a multicast address range, such asFF1E::1-FF1E::2, or both of them, such as FF1E::1, FF1E::10-FF1E::20

delete - Delete multicast address list to or from this multicast VLAN profile. The <mcast_v6address_list> can be a continuous single multicast addresses, such as FF1E::1, a multicast address range, such as FF1E::1-FF1E::2, or both of them, such as FF1E::1, FF1E::10-FF1E::20

<mcast_v6address_list> - Enter the multicast VLAN IPv6 address here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a multicast address or range to an MLD snooping multicast VLAN profile with name “MOD”:

```
DWS-3160-24PC:admin#config mld_snooping multicast_vlan_group_profile MGroup add
FF1E::1, FF1E::10-FF1E::20
Command: config mld_snooping multicast_vlan_group_profile MGroup add FF1E::1,
FF1E::10-FF1E::20

Success.

DWS-3160-24PC:admin#
```

46-5 delete mld_snooping multicast_vlan_group_profile

Description

This command is used to delete an MLD snooping multicast group profile from the Switch.

Format

delete mld_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]

Parameters

profile_name - Specifies the multicast VLAN profile name.

<profile_name 1-32> - Enter the multicast VLAN profile name here. This name can be up to 32 characters long.

all - Specifies to delete all the multicast VLAN profiles.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an MLD snooping multicast group profile with the name “MGroup”:

```
DWS-3160-24PC:admin#delete mld_snooping multicast_vlan_group_profile
profile_name MGroup
Command: delete mld_snooping multicast_vlan_group_profile profile_name MGroup

Success.

DWS-3160-24PC:admin#
```

46-6 show mld_snooping multicast_vlan_group_profile

Description

This command is used to display MLD snooping multicast VLAN group profiles.

Format

show mld_snooping multicast_vlan_group_profile {<profile_name 1-32>}

Parameters

<profile_name 1-32> - (Optional) Enter the multicast VLAN group profile name here. The name can be up to 32 characters long.

If no parameter is specified, then all MLD snooping multicast VLAN group profiles will be displayed.

Restrictions

None.

Example

To display all MLD snooping multicast VLAN group profiles:

```
DWS-3160-24PC:admin#show mld_snooping multicast_vlan_group_profile
Command: show mld_snooping multicast_vlan_group_profile

Profile Name                     Multicast Addresses
-------------------------------- ------------------------------
MGroup                           FF1E::1
                                 FF1E::5
                                 FF1E::10-FF1E::20

 Total Entries: 1

DWS-3160-24PC:admin#
```

46-7 config mld_snooping multicast_vlan_group

Description

This command is used to configure the MLD snooping profile learned with the specific multicast VLAN group.

The following two cases can be considered for examples:

- The multicast group is not configured, multicast VLANs do not have any member ports overlapping and the join packet received by the member port is learned on only the multicast VLAN that this port is a member of.
- The join packet is learned with the multicast VLAN that contains the destination multicast group. If the destination multicast group of the join packet cannot be classified into any multicast VLAN to which this port belongs, then the join packet will be learned on the natural VLAN of the packet.

NOTE: A profile cannot overlap another in different multicast VLANs. Multiple profiles can be added to a multicast VLAN.

Format

config mld_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>

Parameters

<vlan_name 32> - Enter the multicast VLAN name here. The VLAN name can be up to 32 characters long.

add – Specifies to associate an MLD snooping profile to a multicast VLAN.
delete – Specifies to de-associate an MLD snooping profile from a multicast VLAN.

profile_name - Specifies the MLD snooping profile name.
<profile_name 1-32> - Enter the MLD snooping profile name here. The name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add an MLD snooping profile to a multicast VLAN group with the name “mv2”:

```
DWS-3160-24PC:admin#config mld_snooping multicast_vlan_group mv2 add
profile_name MGroup
Command: config mld_snooping multicast_vlan_group mv2 add profile_name MGroup

Success.

DWS-3160-24PC:admin#
```

46-8 show mld_snooping multicast_vlan_group

Description

This command is used to display an MLD snooping multicast VLAN group.

Format

show mld_snooping multicast_vlan_group {<vlan_name 32>}

Parameters

<vlan_name 32> - (Optional) Enter the multicast VLAN name here. This name can be up to 32 characters long.

If no parameter is specified, then all the MLD snooping multicast VLAN groups will be displayed.

Restrictions

None.

Example

To display all MLD snooping multicast VLAN groups configured on the Switch:

```
DWS-3160-24PC:admin#show mld_snooping multicast_vlan_group
Command: show mld_snooping multicast_vlan_group

VLAN Name                        VLAN ID        Multicast Group Profiles
-------------------------------  -------  ---------------------------------
mv2                              4         MGroup

DWS-3160-24PC:admin#
```

46-9 delete mld_snooping multicast_vlan

Description

This command is used to delete an MLD snooping multicast VLAN.

Format

delete mld_snooping multicast_vlan <vlan_name 32>

Parameters

<vlan_name 32> -Enter the multicast VLAN name here. The VLAN name can be up to 32 characters long.	

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an MLD snooping multicast VLAN called “v10”:

```
DWS-3160-24PC:admin#delete mld_snooping multicast_vlan v10
Command: delete mld_snooping multicast_vlan v10

Success.

DWS-3160-24PC:admin#
```

46-10 enable mld_snooping multicast_vlan

Description

This command is used to enable the MLD snooping multicast VLAN function. By default, this features is disabled.

Format

enable mld_snooping multicast_vlan

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the MLD snooping multicast VLAN function globally:

```
DWS-3160-24PC:admin#enable mld_snooping multicast_vlan
Command: enable mld_snooping multicast_vlan

Success.

DWS-3160-24PC:admin#
```

46-11 disable mld_snooping multicast_vlan

Description

This command is used to disable the MLD snooping multicast VLAN function. By default, this features is disabled.

Format

disable mld_snooping multicast_vlan

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the MLD snooping multicast VLAN function:

```
DWS-3160-24PC:admin#disable mld_snooping multicast_vlan
Command: disable mld_snooping multicast_vlan

Success.

DWS-3160-24PC:admin#
```

46-12 config mld_snooping multicast_vlan forward_unmatched

Description

This command is used to configure the forwarding mode for MLD multicast VLAN unmatched packets. When the Switch receives an MLD snooping packet, it will match the packet against the multicast profile to determine which multicast VLAN to associate with it. If the packet does not match all the profiles, the packet will be forwarded or dropped based on this configuration.

Format

config mld_snooping multicast_vlan forward_unmatched [disable | enable]

Parameters

enable – Specifies that the packet will be flooded on the VLAN.
disable – Specifies that the packet will be dropped. This is the default option.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the forwarding mode for MLD multicast VLAN unmatched packets:

```
DWS-3160-24PC:admin#config mld_snooping multicast_vlan forward_unmatched enable
Command: config mld_snooping multicast_vlan forward_unmatched enable

Success.

DWS-3160-24PC:admin#
```

46-13 show mld_snooping multicast_vlan

Description

This command is used to display information for an MLD snooping multicast VLAN.

Format

show mld_snooping multicast_vlan {<vlan_name 32>}

Parameters

<vlan_name 32> - (Optional) Enter the multicast VLAN name here. The VLAN name can be up to 32 characters long.

If no parameter is specified, then all MLD snooping multicast VLAN entries will be displayed.

Restrictions

None.

Example

To display all MLD snooping multicast VLAN entries:

```
DWS-3160-24PC:admin#show mld_snooping multicast_vlan
Command: show mld_snooping multicast_vlan

MLD Multicast VLAN Global State         : Enabled
MLD Multicast VLAN Forward Unmatched    : Enabled

VLAN Name                     :mv2
VID                           :4

Member(Untagged) Ports        :1,3
Tagged Member Ports           :
Source Ports                  :
Untagged Source Ports         :
Status                        :Enabled
Replace Source IP             : ::
Remap Priority                :None

 Total Entries: 1

DWS-3160-24PC:admin#
```

Chapter 47 Multicast Filter Command List

create mcast_filter_profile {[ipv4 | ipv6]} profile_id <value 1-24 > profile_name <name 32>
config mcast_filter_profile [profile_id <value 1-24> | profile_name <name 32>] {profile_name <name 32> | [add | delete] <mcast_address_list>}(1)
config mcast_filter_profile ipv6 [profile_id <value 1-24> | profile_name <name 1-32>] {profile_name <name 1-32> | [add | delete] <mcastv6_address_list>}(1)
delete mcast_filter_profile {[ipv4 | ipv6]} [profile_id [<value 1-24> | all] | profile_name <name 1-32>]
show mcast_filter_profile {[ipv4 | ipv6]} {profile_id <value 1-24> | profile name <name 32>}
config limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} {[add | delete] [profile_id <value 1-24> | profile_name <name 1-32>] | access [permit | deny]}(1)
config max_mcast_group [ports <portlist> | vlanid <vlanid_list] {[ipv4 | ipv6]} {max_group [<value 1-1024> | infinite] | action [drop | replace]}(1)
show max_mcast_group [ports {<portlist>} | vlanid {<vlanid_list >}] {[ipv4 | ipv6]}
show limited_multicast_addr [ports {<portlist>} | vlanid {<vlanid_list>}] {[ipv4 | ipv6]}

47-1 create mcast_filter_profile

Description

This command is used to configure a multicast address profile. Multiple ranges of multicast addresses can be defined in the profile. If the IPv4 or ipv6 option is not specified, IPv4 is implied.

Format

create mcast_filter_profile {[ipv4 | ipv6]} profile_id <value 1-24> profile_name <name 32>

Parameters

ipv4 - (Optional) Adds an IPv4 multicast profile. **ipv6** - (Optional) Adds an IPv6 multicast profile.
profile_id - The ID of the profile. Range is 1 to n. **<value 1-24>** - Enter the profile ID value here. This value must be between 1 and 24.
profile_name - Provides a meaningful description for the profile. **<name 32>** - Enter the profile name here. The profile name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a multicast address profile with a profile ID of 2 and a profile name of MOD:

```
DWS-3160-24PC:admin# create mcast_filter_profile profile_id 2 profile_name MOD
Command: create mcast_filter_profile profile_id 2 profile_name MOD

Success.

DWS-3160-24PC:admin#
```

47-2 config mcast_filter_profile

Description

This command is used to add or delete a range of multicast IP addresses to or from the profile.

Format

config mcast_filter_profile [profile_id <value 1-24> | profile_name <name 32>] {profile_name <name 32> | [add | delete] <mcast_address_list>}(1)

Parameters

profile_id - ID of the profile.
  <value 1-24> - Enter the profile ID value here. This value must be between 1 and 24.

profile_name - Provides a meaningful description for the profile.
  <name 32> - Enter the profile name here. The profile name can be up to 32 characters long.

profile_name - (Optional) Provides a meaningful description for the profile.
  <name 32> - Enter the profile name here. The profile name can be up to 32 characters long.

add - Specifies to add a multicast address.
delete - Specifies to delete a multicast address.

<mcast_address_list> - (Optional) List of the multicast addresses to be put in the profile. You can either Specifies a single multicast IP address or a range of multicast addresses using -.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add the multicast address range 225.1.1.1 to 225.1.1.10 to the profile:

```
DWS-3160-24PC:admin# config mcast_filter_profile profile_id 2 add 225.1.1.1 -
225.1.1.10
Command: config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.10

Success.

DWS-3160-24PC:admin#
```

47-3 config mcast_filter_profile ipv6

Description

This command is used to add or delete a range of IPv6 multicast addresses to the profile.

Format

config mcast_filter_profile ipv6 [profile_id <value 1-24> | profile_name <name 1-32>] {profile_name <name 1-32> | [add | delete] <mcastv6_address_list>}(1)

Parameters

profile_id - ID of the profile.
<value 1-24> - Enter the profile ID value here. This value must be between 1 and 24.

profile_name - Provides a meaningful description for the profile.
<name 1-32> - Enter the profile name here. The profile name can be up to 32 characters long.

profile_name - (Optional) Provides a meaningful description for the profile.
<name 1-32> - Enter the profile name here. The profile name can be up to 32 characters long.

add - (Optional) Specifies to add an IPv6 multicast address.
delete - (Optional) Specifies to delete an IPv6 multicast address.

<mcastv6_address_list> - (Optional) Lists the IPv6 multicast addresses to put in the profile. You can either Specifies a single IPv6 multicast IP address or a range of IPv6 multicast addresses connected by '-'.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add the IPv6 multicast address range FFF0E::100:0:0:20–FFF0E::100:0:0:22 to profile ID 4:

```
DWS-3160-24PC:admin#config mcast_filter_profile ipv6 profile_id 4 add
FF0E::100:0:0:20-FF0E::100:0:0:22
Command: config mcast_filter_profile ipv6 profile_id 4 add FF0E::100:0:0:20-
FF0E::100:0:0:22

Success.

DWS-3160-24PC:admin#
```

47-4 delete mcast_filter_profile

Description

This command is used to delete a multicast address profile. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

delete mcast_filter_profile {[ipv4 | ipv6]} [profile_id [<value 1-24> | all] | profile_name <name 1-32>]

Parameters

ipv4 - (Optional) Specifies to delete an IPv4 multicast profile.
ipv6 - (Optional) Specifies to delete an IPv6 multicast profile.

profile_id - Specifies the ID of the profile
<value 1-24> - Enter the profile ID value here. This value must be between 1 and 24.

all - All multicast address profiles will be deleted.

profile_name - Specifies to display a profile based on the profile name.
<name 1-32> - Enter the profile name value here. The profile name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the multicast address profile with a profile ID of 3:

```
DWS-3160-24PC:admin# delete mcast_filter_profile profile_id 3
Command: delete mcast_filter_profile profile_id 3
Success.

DWS-3160-24PC:admin#
```

To delete the multicast address profile called MOD:

```
DWS-3160-24PC:admin# delete mcast_filter_profile profile_name MOD
Command: delete mcast_filter_profile profile_name MOD

Total entries: 2

DWS-3160-24PC:admin#
```

47-5 show mcast_filter_profile

Description

This command is used to display the defined multicast address profiles. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

show mcast_filter_profile {[ipv4 | ipv6]} {profile_id <value 1-24> | profile name <name 1-32>}

Parameters

ipv4 - (Optional) Specifies to delete an IPv4 multicast profile.
ipv6 - (Optional) Specifies to delete an IPv6 multicast profile.

profile_id - (Optional) Specifies the ID of the profile
<value 1-24> - Enter the profile ID value here. This value must be between 1 and 24.

profile_name - (Optional) Specifies to display a profile based on the profile name.
<name 1-32> - Enter the profile name here. The profile name can be up to 32 characters long.

Restrictions

None.

Example

To display all the defined multicast address profiles:

```
DWS-3160-24PC:admin#show mcast_filter_profile
Command: show mcast_filter_profile

Profile ID Name                             Multicast Addresses
---------- -------------------------------- -------------------------------
2          MOD                              225.1.1.1-225.1.1.10
                                            234.1.1.1-238.244.244.244

Total Entries: 1

DWS-3160-24PC:admin#
```

47-6 config limited_multicast_addr

Description

This command is used to configure the multicast address filtering function on a port or VLAN. When there are no profiles specified with a port or VLAN, the limited function is not effective. When the function is configured on a port, it limits the multicast group operated by the IGMP or MLD snooping function. When this function is configured on a VLAN, the multicast group is limited to only operate the IGMP or MLD Layer 3 functions. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

config limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} {[add | delete] [profile_id <value 1-24> | profile_name <name 1-32>] | access [permit | deny]}(1)

Parameters

ports - Specifies the range of ports to configure the multicast address filtering function.
<portslist> - Enter the list of port to be configured here.

vlanid - Specifies the VLAN ID of the VLAN that the multicast address filtering function will be configured on.
<vlanid_list> - Enter the VLAN ID list here.

ipv4 - (Optional) Specifies the IPv4 multicast profile.
ipv6 - (Optional) Specifies the IPv6 multicast profile.

add - (Optional) Adds a multicast address profile to a port.
delete - (Optional) Deletes a multicast address profile to a port.

profile_id - (Optional) A profile to be added to or deleted from the port
<value 1-24> - Enter the profile ID value here. This value must be between 1 and 24.

profile_name - (Optional) Specifies the profile name used.
<name 1-32> - Enter the profile name here. The profile name can be up to 32 characters long.

access - (Optional) Specifies the access of packets matching the addresses defined in the profiles.
permit - Specifies that packets matching the addresses defined in the profiles will be permitted. The default mode is permit.
deny - Specifies that packets matching the addresses defined in the profiles will be denied.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add multicast address profile 2 to ports 1 and 3:

```
DWS-3160-24PC:admin# config limited_multicast_addr ports 1,3 add profile_id 2
Command: config limited_multicast_addr ports 1,3 add profile_id 2

Success.

DWS-3160-24PC:admin#
```

47-7 config max_mcast_group

Description

This command is used to configure the maximum number of multicast groups that a port can join. If the IPv4 or IPv6 option is not specified, IPv4 is implied. When the joined groups for a port or a VLAN have reached the maximum number, the newly learned group will be dropped if the action is specified as drop. The newly learned group will replace the eldest group if the action is specified as replace.

Format

config max_mcast_group [ports <portlist> | vlanid <vlanid_list] {[ipv4 | ipv6]} {max_group [<value 1-1024> | infinite] | action [drop | replace]}(1)

Parameters

ports - Specifies the range of ports to configure the max_mcast_group.
  <portlist> - Enter the list of ports to be configured here.

vlanid - Specifies the VLAN ID to configure max_mcast_group.
  <vlanid_list> - Enter the VLAN ID list here.

ipv4 - (Optional) Specifies that the maximum number of IPv4 learned addresses should be limited.
ipv6 - (Optional) Specifies that the maximum number of IPv6 learned addresses should be limited.

max_group - (Optional) Specifies the maximum number of multicast groups.
  <value 1-1024> - Enter the maximum group value here. This value must be between 1 and 1024.
  infinite - Specifies that the maximum group value will be set to infinite.

action - (Optional) Specifies the action for handling newly learned groups when the register is full.
  drop - The new group will be dropped.
  replace - The new group will replace the eldest group in the register table.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the maximum number of multicast group that ports 1 and 3 can join to 100:

```
DWS-3160-24PC:admin#config max_mcast_group ports 1, 3 max_group 100
Command: config max_mcast_group ports 1,3 max_group 100

Success.

DWS-3160-24PC:admin#
```

47-8 show max_mcast_group

Description

This command is used to display the maximum number of multicast groups that a port can join. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

show max_mcast_group [ports {<portlist>} | vlanid {<vlanid_list >}] {[ipv4 | ipv6]}

Parameters

ports - Specifies the range of ports for displaying information about the maximum number of multicast groups that the specified ports can join.
<portlist> - (Optional) Enter the list of ports to be configured here.

vlanid - Specifies the VLAN ID for displaying the maximum number of multicast groups.
<vlanid_list> - (Optional) Enter the VLAN ID list here.

ipv4 - (Optional) Specifies to display the maximum number of IPv4 learned addresses.
ipv6 - (Optional) Specifies to display the maximum number of IPv6 learned addresses.

Restrictions

None.

Example

To display the maximum number of multicast groups that ports 1 to 3 can join:

```
DWS-3160-24PC:admin#show max_mcast_group ports 1-3
Command: show max_mcast_group ports 1-3

Port      Max Multicast Group Number    Action
------    ----------------------------  ---------
1         100                             Drop
2         Infinite                        Drop
3         100                             Drop

Total Entries: 3

DWS-3160-24PC:admin#
```

To display the maximum number of multicast groups that VLANs 1 to 3 can join:

```
DWS-3160-24PC:admin#show max_mcast_group vlanid 1-3
Command: show max_mcast_group vlanid 1-3

VLAN      Max Multicast Group Number    Action
------    ----------------------------  ---------
1         Infinite                        Drop
2         Infinite                        Drop
3         Infinite                        Drop

Total Entries: 3

DWS-3160-24PC:admin#
```

47-9 show limited_multicast_addr

Description

This command is used to display the multicast address range by port or by VLAN. When the function is configured on a port, it limits the multicast groups operated by the IGMP or MLD snooping function and Layer 3 functions. When the function is configured on a VLAN, it limits the multicast groups operated by the IGMP or MLD Layer 3 functions.

If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

show limited_multicast_addr [ports {<portlist>} | vlanid {<vlanid_list>}] {[ipv4 | ipv6]}

Parameters

ports - Specifies the range of ports that require information displaying about the multicast address filtering function.
<portlist> - (Optional) Enter the list of port to be configured here.

vlanid - Specifies the VLAN ID of VLANs that require information displaying about the multicast address filtering function.
<vlanid_list> - (Optional) Enter the VLAN ID list here.

ipv4 - (Optional) Specifies to display the IPv4 multicast profile associated with the port.
ipv6 - (Optional) Specifies to display the IPv6 multicast profile associated with the port.

Restrictions

None.

Example

To display the limited multicast address range on ports 1 and 3:

```
DWS-3160-24PC:admin#show limited_multicast_addr ports 1,3
Command: show limited_multicast_addr ports 1,3

Port    : 1
Access  : Deny

Profile ID Name                             Multicast Addresses
---------- -------------------------------- -------------------------------
2          MOD                              225.1.1.1-225.1.1.10
                                            234.1.1.1-238.244.244.244


Port    : 3
Access  : Deny

Profile ID Name                             Multicast Addresses
---------- -------------------------------- -------------------------------
2          MOD                              225.1.1.1-225.1.1.10
                                            234.1.1.1-238.244.244.244

DWS-3160-24PC:admin#
```

Chapter 48 Multiple Spanning Tree Protocol (MSTP) Command List

show stp

show stp instance {<value 0-15>}

show stp ports {<portlist>}

show stp mst_config_id

create stp instance_id <value 1-15>

delete stp instance_id <value 1-15>

config stp instance_id <value 1-15> [add_vlan | remove_vlan] <vidlist>

config stp mst_config_id {revision_level <int 0-65535> | name <string>}

enable stp

disable stp

config stp version [mstp | rstp | stp]

config stp priority <value 0-61440> instance_id <value 0-15>

config stp {maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] | nni_bpdu_addr [dot1d | dot1ad]}

config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] |edge [true | false | auto] | p2p [true | false | auto] | state [enable | disable] | restricted_role [true | false] | restricted_tcn [true | false] | fbpdu [enable | disable]}

config stp mst_ports <portlist> instance_id <value 0-15> {internalCost [auto | <value 1-200000000>] | priority <value 0-240>}

48-1 show stp

Description

This command is used to display the global configuration of the Spanning Tree Protocol (STP).

Format

show stp

Parameters

None.

Restrictions

None.

Example

To display STP:

```
DWS-3160-24PC:admin#show stp
Command: show stp

 STP Bridge Global Settings
 ---------------------------
 STP Status         : Disabled
 STP Version        : RSTP
 Max Age            : 20
 Hello Time         : 2
 Forward Delay      : 15
 Max Hops           : 20
 TX Hold Count      : 6
 Forwarding BPDU    : Disabled
 NNI BPDU Address   : dot1d

DWS-3160-24PC:admin#
```

48-2 show stp instance

Description

This command is used to displays each STP instance configuration.

Format

show stp instance {<value 0-15>}

Parameters

instance - Specifies the MSTP instance ID.

<value 0-15> - (Optional) Enter the MSTP instance ID value here. This value must be between 0 and 15.

Restrictions

None.

Example

To display STP instance:

```
DWS-3160-24PC:admin#show stp instance
Command: show stp instance

 STP Instance Settings
 ---------------------------
 Instance Type          : CIST
 Instance Status        : Enabled
 Instance Priority      : 61440(Bridge Priority : 61440, SYS ID Ext : 0 )

 STP Instance Operational Status
 --------------------------------
 Designated Root Bridge : 61440/00-11-22-33-45-67
 External Root Cost     : 0
 Regional Root Bridge   : 61440/00-11-22-33-45-67
 Internal Root Cost     : 0
 Designated Bridge      : 61440/00-11-22-33-45-67
 Root Port              : None
 Max Age                : 25
 Forward Delay          : 15
 Last Topology Change   : 22
 Topology Changes Count : 1

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

48-3 show stp ports

Description

This command is used to display the port information includes parameters setting and operational value.

Format

show stp ports {<portlist>}

Parameters

ports - To display parameters of the designated port numbers, to be distinguished from displaying parameters of the bridge.
<portlist> - (Optional) Enter a list of ports used for the configuration here.

Restrictions

None.

Example

To display STP ports:

```
DWS-3160-24PC:admin#show stp ports
Command: show stp ports

 MSTP Port Information
 ----------------------
 Port Index     : 1     , Hello Time: 2 /2 , Port STP : Enabled  ,
 External PathCost : Auto/20000    , Edge Port : False/No , P2P : Auto /Yes
 Port RestrictedRole : False,  Port RestrictedTCN : False
 Port Forward BPDU : Disabled
 MSTI   Designated Bridge   Internal PathCost  Prio  Status      Role
 -----  ------------------  -----------------  ----  ----------  ----------
 0      F000/001122334567   20000              128   Forwarding  Designated
 2      8002/001122334567   20000              128   Forwarding  Designated

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

48-4 show stp mst_config_id

Description

This command is used to display the MST configuration identification.

Format

show stp mst_config_id

Parameters

None.

Restrictions

None.

Example

To display STP MST configuration ID:

```
DWS-3160-24PC:admin#show stp mst_config_id
Command: show stp mst_config_id

 Current MST Configuration Identification
 ----------------------------------------

 Configuration Name : R&D_BlockG                        Revision Level :1
 MSTI ID     VID List
 -------     -------------------------------------------------------------
    CIST     4-4094
       2     1-3

DWS-3160-24PC:admin#
```

48-5 create stp instance_id

Description

This command is used to create an MST Instance without mapping the corresponding VLANs.

Format

create stp instance_id <value 1-15>

Parameters

instance_id - Specifies the MSTP instance ID. Instance 0 represents for default instance, CIST.

<value 1-15> - Enter the MSTP instance ID here. This value must be between 1 and 15.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create MSTP instance:

```
DWS-3160-24PC:admin#create stp instance_id 2
Command: create stp instance_id 2

 Warning:There is no VLAN mapping to this instance_id!
Success.

DWS-3160-24PC:admin#
```

48-6 delete stp instance_id

Description

This command is used to delete an MST Instance.

Format

delete stp instance_id <value 1-15>

Parameters

instance_id - Specifies the MSTP instance ID. Instance 0 represents for default instance, CIST.

<value 1-15> - Enter the MSTP instance ID here. This value must be between 1 and 15.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an MSTP instance:

```
DWS-3160-24PC:admin# delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DWS-3160-24PC:admin#
```

48-7 config stp instance_id

Description

This command is used to map or remove the VLAN range of the specified MST instance for the existed MST instances.

Format

config stp instance_id <value 1-15> [add_vlan | remove_vlan] <vidlist>

Parameters

instance_id - Specifies the MSTP instance ID. Instance 0 represents for default instance, CIST.

  <value 1-15> - Enter the MSTP instance ID here. This value must be between 1 and 15.

add_vlan - Specifies to map the specified VLAN list to an existing MST instance.

remove_vlan - Specifies to delete the specified VLAN list from an existing MST instance.

<vidlist> - Specifies a list of VLANs by VLAN ID.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To map a VLAN ID to an MSTP instance:

```
DWS-3160-24PC:admin# config stp instance_id 2 add_vlan 1-3
Command: config stp instance_id 2 add_vlan 1-3

Success.

DWS-3160-24PC:admin#
```

To remove a VLAN ID from an MSTP instance:

```
DWS-3160-24PC:admin# config stp instance_id 2 remove_vlan 2
Command: config stp instance_id 2 remove_vlan 2

Success.

DWS-3160-24PC:admin#
```

48-8 config stp mst_config_id

Description

This command is used to change the name or the revision level of the MST configuration identification.

Format

config stp mst_config_id {revision_level <int 0-65535> | name <string>}

Parameters

name - (Optional) Specifies the name given for a specific MST region.
<string> - Enter the MST region name here.

revision_level - (Optional) The same given name with different revision level also represents different MST regions.
<int 0-65535> - Enter the revision level here. This value must be between 0 and 65535.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To change the name and revision level of the MST configuration identification:

```
DWS-3160-24PC:admin# config stp mst_config_id name R&D_BlockG revision_level 1
Commands: config stp mst_config_id name R&D_BlockG revision_level 1

Success.

DWS-3160-24PC:admin#
```

48-9 enable stp

Description

This command is used to enable STP globally.

Format

enable stp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable STP:

```
DWS-3160-24PC:admin# enable stp
Command: enable stp

Success.

DWS-3160-24PC:admin#
```

48-10 disable stp

Description

This command is used to disable STP globally.

Format

disable stp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable STP:

```
DWS-3160-24PC:admin# disable stp
Command: disable stp

Success.

DWS-3160-24PC:admin#
```

48-11 config stp version

Description

This command is used to configure the STP version used.

Format

config stp version [mstp | rstp | stp]

Parameters

version – Specifies that the STP version will be configured.
mstp – Specifies that the STP version will be configured as Multiple Spanning Tree Protocol.
rstp - Specifies that the STP version will be configured as Rapid Spanning Tree Protocol.
stp - Specifies that the STP version will be configured as Spanning Tree Protocol.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the STP version:

```
DWS-3160-24PC:admin# config stp version mstp
Command: config stp version mstp

Success.

DWS-3160-24PC:admin#
```

To configure the STP version with the same value of old configuration:

```
DWS-3160-24PC:admin# config stp version mstp
Command: config stp version mstp

Configure value is the same with current value.
Success.

DWS-3160-24PC:admin#
```

48-12 config stp priority

Description

This command is used to configure the STP instance’s priority.

Format

config stp priority <value 0-61440> instance_id <value 0-15>

Parameters

priority - Specifies the bridge priority value. This value must be divisible by 4096.
<value 0-61440> - Enter the bridge priority value here. This value must be between 0 and 61440.

instance_id - Identifier to distinguish different STP instances.
<value 0-15> - Enter the STP instance ID here. This value must be between 0 and 15.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the STP instance's priority:

```
DWS-3160-24PC:admin# config stp priority 61440 instance_id 0
Command: config stp priority 61440 instance_id 0

Success.

DWS-3160-24PC:admin#
```

48-13 config stp

Description

This command is used to configure the STP parameter settings.

Format

config stp {maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] | nni_bpdu_addr [dot1d | dot1ad]}

Parameters

maxage - (Optional) Used to determine if a BPDU is valid. The default value is 20.

<value 6-40> - Enter the maximum age value here. This value must be between 6-40.

maxhops - (Optional) Used to restrict the forwarded times of one BPDU. The default value is 20.

<value 6-40> - Enter the maximum hops value here. This value must be between 6 and 40.

hello_time - (Optional) The time interval for sending configuration BPDUs by the Root Bridge. The default value is 2 seconds. This parameter is for STP and RSTP version. MSTP version uses per-port hellotime parameter.

<value 1-2> - Enter the hello time value here. This value must be between 1 and 2.

forwarddelay - (Optional) The maximum delay time for one BPDU to be transmitted by a bridge and received from another bridge. The default value is 15.

<value 4-30> - Enter the maximum delay time here. This value must be between 4 and 30.

txholdcount - (Optional) Used to restrict the numbers of BPDU transmitted in a time interval.

<value 1-10> - Enter the transmitted BPDU restriction value here. This value must be between 1 and 10.

fbpdu - (Optional) To decide if the bridge will flood STP BPDU when STP functionality is disabled.

enable - Specifies that the bridge will flood STP BPDU when STP functionality is disabled

disable - Specifies that the bridge will not flood STP BPDU when STP functionality is disabled

nni_bpdu_addr - (Optional) Used to determine the BPDU protocol address for GVRP in service provide site. It can use 802.1d GVRP address, 802.1ad service provider GVRP address or an user defined multicast address. The range of the user defined address is 0180C2000000 - 0180C2FFFFFF.

dot1d - Specifies that the NNI BPDU protocol address value will be set to Dot1d.

dot1ad - Specifies that the NNI BPDU protocol address value will be set to Dot1ad.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure STP:

```
DWS-3160-24PC:admin# config stp maxage 25
Command: config stp maxage 25

Success.

DWS-3160-24PC:admin#
```

48-14 config stp ports

Description

This command is used to configure STP parameters for each port, except for Internal Path Cost and Port Priority.

Format

config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] | edge [true | false | auto] | p2p [true | false | auto] | state [enable | disable]| restricted_role [true | false] | restricted_tcn [true | false] | fbpdu [enable | disable]}

Parameters

<portlist> - Enter a list of ports used for the configuration here.

external_cost - (Optional) The path cost between MST regions from the transmitting Bridge to the CIST Root Bridge. It is only used at CIST level.
- **auto** - Specifies that the external cost value will be set to automatic.
- **<value 1-200000000>** - Enter the external cost value here. This value must be between 1 and 200000000.

hellotime - (Optional) The default value is 2 . This parameter is for MSTP version. For STP and RSTP version, uses the per system hellotime parameter.
- **<value 1-2>** - Enter the hello time value here. This value must be between 1 and 2.

migrate - (Optional) Operation of management in order to Specifies the port to send MSTP BPDU for a delay time.
- **yes** - Specifies that the MSTP BPDU for a delay time will be sent.
- **no** - Specifies that the MSTP BPDU for a delay time will not be sent.

edge - (Optional) To decide if this port is connected to a LAN or a Bridged LAN.
- **true** - Specifies that the specified port(s) is edge.
- **false** - Specifies that the specified port(s) is not edge.
- **auto** - In auto mode, the bridge will delay for a period to become edge port if no bridge BPUD is received. The default is auto mode.

p2p - (Optional) To decide if this port is in Full-Duplex or Half-Duplex mode.
- **true** - Specifies that the port(s) is in Full-Duplex mode.
- **false** - Specifies that the port(s) is in Half-Duplex mode.
- **auto** - Specifies that the port(s) is in Full-Duplex and Half-Duplex mode.

state - (Optional) To decide if this port supports the STP functionality.
- **enable** - Specifies that STP functionality on the port(s) is enabled.
- **disable** - Specifies that STP functionality on the port(s) is disabled.

restricted_role - (Optional) To decide if this port not to be selected as Root Port. The default value is false.
- **true** - Specifies that the port can be specified as the root port.
- **false** - Specifies that the port cannot be specified as the root port.

restricted_tcn - (Optional) To decide if this port not to propagate topology change. The default value is false.

true - Specifies that the port can be set to propagate a topology change.
false - Specifies that the port cannot be set to propagate a topology change.

fbpdu - (Optional) To decide if this port will flood STP BPDU when STP functionality is disabled. When the state is set to enable, the received BPDU will be forwarded. When the state is set to disable, the received BPDU will be dropped.
enable - Specifies that the port can be set to flood the STP BPDU when the STP functionality is disabled.
disable - Specifies that the port cannot be set to flood the STP BPDU when the STP functionality is disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure STP ports:

```
DWS-3160-24PC:admin# config stp ports 1 externalCost auto
Command: config stp ports 1 externalCost auto

Success.

DWS-3160-24PC:admin#
```

48-15 config stp mst_ports

Description

This command is used to configure the ports management parameters.

Format

config stp mst_ports <portlist> instance_id <value 0-15> {internalCost [auto | <value 1-200000000>] | priority <value 0-240>}

Parameters

mst_ports - Specifies to be distinguished from the parameters of ports only at CIST level.
<portlist> - Enter a list of ports used for the configuration here.

instance_id - Specifies the instance ID used.
<value 0-15> - Enter the instance ID used here. This value must be between 0 and 15.

internalCost - (Optional) Specifies the port path cost used in MSTP.
auto - Specifies that the internal cost value will be set to auto.
<value 1-200000000> - Enter the internal cost value here. This value must be between 1 and 200000000.

priority - (Optional) Specifies the port priority value.
<value 0-240> - Enter the port priority value here. This value must be between 0 and 240.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure STP MST ports:

```
DWS-3160-24PC:admin# config stp mst_ports 1 instance_id 0 internalCost auto
Command: config stp mst_ports 1 instance_id 0 internalCost auto

Success.

DWS-3160-24PC:admin#
```

Chapter 49 Network Load Balancing (NLB) Command List

create nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>
delete nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>
config nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr> [add | delete] <portlist>
show nlb fdb

49-1 create nlb multicast_fdb

Description

This command is used to create a Network Load Balancing (NLB) multicast FDB entry. This command supports the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all servers, but will only be processed by one of them. The server can work in two different modes – unicast mode and multicast mode. In unicast mode, the client use unicast MAC address as the destination MAC to reach the server. In multicast mode, the client use the multicast MAC address as the destination MAC to reach the server. Regarding of the mode, this destination MAC is the named the shared MAC. The server uses its own MAC address (rather than the shared MAC) as the source MAC address of the reply packet.

The NLB multicast FDB entry will be mutual exclusive with the Layer 2 multicast entry.

Format

create nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>

Parameters

multicast_fdb - Specifies the VLAN of the NLB multicast FDB entry to be created. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the VLAN by the VLAN ID. **<vlanid>** - Enter the VLAN ID here.
<macaddr> - Specifies the MAC address of the NLB multicast FDB entry to be created.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a NLB multicast FDB entry:

```
DWS-3160-24PC:admin# create nlb multicast_fdb default 03-bf-01-01-01-01
Command: create nlb multicast_fdb default 03-bf-01-01-01-01

Success.

DWS-3160-24PC:admin#
```

49-2 delete nlb multicast_fdb

Description

This command is used to delete an NLB multicast FDB entry.

Format

delete nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>

Parameters

<vlan_name 32> - Specifies the VLAN of the NLB multicast FDB entry to be deleted.
vlanid - Specifies the VLAN by VLAN ID. **<vlanid>** - Enter the VLAN ID here.
<macaddr> - Specifies the MAC address of the NLB multicast FDB entry to be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an NLB multicast FDB entry:

```
DWS-3160-24PC:admin# delete nlb multicast_fdb default 03-bf-01-01-01-01
Command: delete nlb multicast_fdb default 03-bf-01-01-01-01

Success.

DWS-3160-24PC:admin#
```

49-3 config nlb multicast_fdb

Description

This command is used to add or delete forwarding ports to or from the specified NLB multicast FDB entry.

Format

config nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr> [add | delete] <portlist>

Parameters

<vlan_name 32> - Specifies the VLAN of the NLB multicast FDB entry to be configured.
vlanid - Specifies the VLAN by the VLAN ID.
<vlanid> - Enter the VLAN ID here.

<macaddr> - Specifies the MAC address of the NLB multicast FDB entry to be configured.
add - Specifies a list of forwarding ports to be added.
delete - Specifies a list of forwarding ports to be deleted.

<portlist> - Enter the list of ports used for this configuration.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure NLB multicast MAC forwarding database:

```
DWS-3160-24PC:admin# config nlb multicast_fdb default 03-bf-01-01-01-01 add 1-5
Command: config nlb multicast_fdb default 03-bf-01-01-01-01 add 1-5

Success.

DWS-3160-24PC:admin#
```

49-4 show nlb fdb

Description

This command is used to display the NLB configured entry table.

Format

show nlb fdb

Parameters

None.

Restrictions

None.

Example

To display the NLB forwarding table:

```
DWS-3160-24PC:admin#show nlb fdb
Command: show nlb fdb

 MAC Address       VLAN ID    Egress Ports
 ----------------- ---------- ---------------------------------------------
 03-BF-01-01-01-01 1          1-5

Total Entries :1

DWS-3160-24PC:admin#
```

Chapter 50 Network Monitoring Command List

show packet ports <portlist>
show error ports <portlist>
show utilization [cpu | ports]
show utilization dram
show utilization flash
clear counters {ports <portlist>}

50-1 show packet ports

Description

This command is used to display statistics about the packets sent and received by the Switch.

Format

show packet ports <portlist>

Parameters

<portlist> - Specifies a range of ports to be displayed.

Restrictions

None.

Example

To display the packets analysis for port 23:

```
DWS-3160-24PC:admin#show packet ports 23
Command: show packet ports 23

 Port Number : 23
 ==================================================================
 Frame Size/Type      Frame Counts                 Frames/sec
 ---------------      ----------------------       -----------
 64                   626                          0
 65-127               360                          0
 128-255              116                          0
 256-511              189                          0
 512-1023             40                           0
 1024-1518            55                           0
 Unicast RX           603                          0
 Multicast RX         37                           0
 Broadcast RX         40                           0

 Frame Type           Total                        Total/sec
 ---------------      ----------------------       -----------
 RX Bytes             92853                        0
 RX Frames            680                          0
 TX Bytes             682310                       0
 TX Frames            1042                         0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

50-2 show error ports

Description

This command is used to display error statistics for a range of ports.

Format

show errors ports <portlist>

Parameters

<portlist> - Specifies a range of ports to be displayed.

Restrictions

None.

Example

To display the errors of the port 23

```
DWS-3160-24PC:admin#show error ports 23
Command: show error ports 23

 Port Number : 23
                RX Frames                              TX Frames
                ---------                              ---------
 CRC Error      0                  Excessive Deferral    0
 Undersize      0                  CRC Error             0
 Oversize       0                  Late Collision        0
 Fragment       0                  Excessive Collision   0
 Jabber         0                  Single Collision      0
 Drop Pkts      11                 Collision             0
 Symbol Error   0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

50-3 show utilization

Description

This command is used to display real-time CPU or port utilization statistics.

Format

show utilization [cpu | ports]

Parameters

cpu - Specifies to display information regarding the CPU.
ports - Specifies a range of ports to be displayed.

Restrictions

None.

Example

To display the ports utilization:

```
DWS-3160-24PC:admin#show utilization ports
Command: show utilization ports

 Port     TX/sec     RX/sec    Util      Port     TX/sec     RX/sec    Util
 -----  ---------- ---------- ----      -----  ---------- ---------- ----
 1      0          0          0         21     0          0          0
 2      0          0          0         22     0          0          0
 3      0          0          0         23     0          0          1
 4      0          0          0         24     0          0          0
 5      0          0          0
 6      0          0          0
 7      0          0          0
 8      0          0          0
 9      0          0          0
 10     0          0          0
 11     0          0          0
 12     0          0          0
 13     0          0          0
 14     0          0          0
 15     0          0          0
 16     0          0          0
 17     0          0          0
 18     0          0          0
 19     0          0          0
 20     0          0          0
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

To display the CPU utilization:

```
DWS-3160-24PC:admin#show utilization cpu
Command: show utilization cpu

CPU Utilization
-------------------------------------------------------------------------------
Five seconds -  11 %         One minute -  11 %         Five minutes -  11 %


DWS-3160-24PC:admin#
```

50-4 show utilization dram

Description

This command is used to display DRAM memory utilization.

Format

show utilization dram

Parameters

None.

Restrictions

None.

Example

To display DRAM utilization:

```
DWS-3160-24PC:admin#show utilization dram
Command: show utilization dram

DRAM utilization :
        Total DRAM      : 262144    KB
        Used DRAM       : 232732    KB
        Utilization     : 88 %



CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

50-5 show utilization flash

Description

This command is used to display the flash memory utilization.

Format

show utilization flash

Parameters

None.

Restrictions

None.

Example

To display FLASH utilization:

```
DWS-3160-24PC:admin#show utilization flash
Command: show utilization flash

Flash Memory Utilization :
        Total Flash     : 29618     KB
        Used Flash      : 8251      KB
        Utilization     : 27 %


CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

50-6 clear counters

Description

This command is used to clear the Switch’s statistics counters.

Format

clear counters {ports <portlist>}

Parameters

ports - (Optional) Specifies a range of ports to be configured. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then highest Switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash.
<portlist> - Enter a list of ports used for the configuration here.

If no parameter is specified, system will display counters of all the ports .

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the Switch’s statistics counters:

```
DWS-3160-24PC:admin# clear counters ports 7-9
Command: clear counters ports 7-9

Success.

DWS-3160-24PC:admin#
```

Chapter 51 OAM Command List

config ethernet_oam ports [<portlist> | all] [mode [active | passive] | state [enable | disable] | link_monitor [error_symbol {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]}(1) | error_frame {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]}(1) | error_frame_seconds {threshold <range 1-900> | window <millisecond 10000-900000> | notify_state [enable | disable]}(1) | error_frame_period {threshold <range 0-4294967295> | window <number 148810-100000000> | notify_state [enable | disable]}(1)] | critical_link_event [dying_gasp | critical_event] notify_state [enable | disable] | remote_loopback [start | stop] | received_remote_loopback [process | ignore]]

show ethernet_oam ports {<portlist>} [status | configuration | statistics | event_log {index <value_list>}]

clear ethernet_oam ports [<portlist> | all] [event_log | statistics]

51-1 config ethernet_oam ports

Description

This command is used to configure Ethernet Operations, Administration, and Maintenance (OAM). The user can configure each port’s Ethernet OAM mode to operate in the active or passive mode.

The following two actions are allowed, per port, in the active mode, but not allowed, per port, in the passive mode:

- Initiate OAM discovery.
- Start or stop remote loopback.

NOTE: When a port is OAM-enabled, changing the OAM mode will cause the OAM discovery to restart.

This command is also used to enable or disable a port’s Ethernet OAM function. Enabling a port’s OAM will cause the port, if active, to start the OAM discovery or it will react to a discovery packet received from the peer. Disabling a port’s OAM will cause the port to send out a dying gasp event to peers and then disconnect the established OAM link.

The link monitoring parameter is used to configure a port’s Ethernet OAM link monitoring error symbols. The link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM will monitor the statistics on the number of frame errors as well as the number of coding symbol errors. When the number of symbol errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it will generate an error symbol period event to notify the remote OAM peer. The Ethernet OAM link monitoring error frames parameter provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the counter on the number of frame errors as well as the number of coding symbol errors. When the number of frame errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame event to notify the remote OAM peer.

The link event parameter configures the capability of the Ethernet OAM critical link event. If the capability for an event is disabled, the port will never send out the corresponding critical link event. The command is used to configure the client to process or to ignore the received Ethernet OAM remote loopback command. In remote loopback mode, all user traffic will not be processed. Ignoring the received remote loopback command will prevent the port from entering remote loopback mode.

Format

config ethernet_oam ports [<portlist> | all] [mode [active | passive] | state [enable | disable] | link_monitor [error_symbol {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]} (1) | error_frame {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]} (1) | error_frame_seconds {threshold <range 1-900> | window <millisecond 10000-900000> | notify_state [enable | disable]} (1) | error_frame_period {threshold <range 0-4294967295> | window <number 148810-100000000> | notify_state [enable | disable]}(1)] | critical_link_event [dying_gasp | critical_event] notify_state [enable | disable] | remote_loopback [start | stop] | received_remote_loopback [process | ignore]]

Parameters

<portlist> - Used to Specifies a range of ports to be configured.
all - Specifies the all ports are to be configured.
mode - Specifies the operation mode. The default mode is active. **active** - Specifies to operate in active mode. **passive** - Specifies to operate in passive mode.
state - Specifies the OAM function status. **enable** - Specifies to enable the OAM function. **disable** - Specifies to disable the OAM function.
link_monitor - Used to detect and indicate link faults under a variety of conditions. **error_symbol** - Used to generate an error symbol period event to notify the remote OAM peer. **threshold** - Specifies the number of symbol errors in the period that is required to be equal to or greater than in order for the event to be generated. The default value of threshold is 1 symbol error. **<range 0-4294967295>** - Specifies the range from 0 to 4294967295. **window** - The range is 1000 to 60000ms. The default value is 1000ms. **<millisecond 1000-60000>** -The range is 1000 to 60000ms. **notify_state** - Specifies the event notification status. The default state is enabled. **enable** -Specifies to enable event notification. **disable** -Specifies to disable event notification. **error_frame** - Specifies the error frame. **threshold** - Specifies a threshold range. **<range 0-4294967295>** - Specifies a threshold range between 0 and 4294967295. **window** - The range is 1000 to 60000ms. The default value is 1000ms. **<millisecond 1000-60000>** - The range is 1000 to 60000ms. **notify_state** - Specifies the event notification status. The default state is enabled. **enable** - Specifies to enable event notification. **disable** - Specifies to disable event notification. **error_frame_seconds** - Specifies error frame time. **threshold** - Specifies a threshold range between 1 and 900. **<range 1-900>** -Specifies a threshold range between 1 and 900. **window** - The range is 1000 to 900000ms. **<millisecond 10000-900000> -** The range is 1000 to 900000ms. **notify_state** - Specifies the event notification status. The default state is enabled. **enable** - Specifies to enable event notification.

disable - Specifies to disable event notification. **error_frame_period** - Specifies error frame period. **threshold** - Specifies a threshold range between 0 and 4294967295. **<range 0-4294967295>** -Specifies a threshold range between 0 and 4294967295. **window** - The range is 148810 to 100000000ms. **<number 148810-100000000>** - The range is 148810 to 100000000ms. **notify_state** - Specifies the event notification status. The default state is enabled. **enable** - Specifies to enable event notification. **disable** - Specifies to disable event notification.
critical_link_event –Specifies critical link event. **dying_gasp** - An unrecoverable local failure condition has occurred. **critical_event** - An unspecified critical event has occurred. **notify_state** - Specifies the event notification status. The default state is enabled. **enable** - Specifies to enable event notification. **disable** - Specifies to disable event notification.
remote_loopback - Specifies remote loop. **start** - If start is specified, it will request the peer to change to the remote loopback mode. **stop** - If stop is specified, it will request the peer to change to the normal operation mode.
received_remote_loopback - Specifies receive remote loop-back. **process** - Specifies to process the received Ethernet OAM remote loopback command. **ignore** - Specifies to ignore the received Ethernet OAM remote loopback command. The default method is ignore”.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure Ethernet OAM on ports 1 to 2 in active mode:

```
DWS-3160-24PC:admin# config ethernet_oam ports 1-2 mode active
Command: config ethernet_oam ports 1-2 mode active

Success.

DWS-3160-24PC:admin#
```

To enable Ethernet OAM on port 1:

```
DWS-3160-24PC:admin# config ethernet_oam ports 1 state enable
Command: config ethernet_oam ports 1 state enable

Success.

DWS-3160-24PC:admin#
```

To configure the error symbol threshold to 2 and period to 1000ms for port 1:

```
DWS-3160-24PC:admin# config ethernet_oam ports 1 link_monitor error_symbol
threshold 2 window 1000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_symbol threshold 2
window 1000 notify_state enable

Success.
```

```

DWS-3160-24PC:admin#
```

To configure the error frame threshold to 2 and period to 1000 ms for port 1:

```
DWS-3160-24PC:admin# config ethernet_oam ports 1 link_monitor error_frame
threshold 2 window 1000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame threshold 2
window 1000 notify_state enable

Success.

DWS-3160-24PC:admin#
```

To configure the error frame seconds threshold to 2 and period to 10000 ms for port 1:

```
DWS-3160-24PC:admin# config ethernet_oam ports 1 link_monitor
error_frame_seconds threshold 2 window 10000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame_seconds threshold
2 window 10000 notify_state enable

Success.

DWS-3160-24PC:admin#
```

To configure the error frame threshold to10 and period to 1000000 ms for port 1:

```
DWS-3160-24PC:admin# config ethernet_oam ports 1 link_monitor
error_frame_period threshold 10 window 1000000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame_period threshold
10 window 1000000 notify_state enable

Success.

DWS-3160-24PC:admin#
```

To configure a dying gasp event for port 1:

```
DWS-3160-24PC:admin# config ethernet_oam ports 1 critical_link_event dying_gasp
notify_state enable
Command: config ethernet_oam ports 1 critical_link_event dying_gasp
notify_state enable

Success.

DWS-3160-24PC:admin#
```

To start remote loopback on port 1:

```
DWS-3160-24PC:admin# config ethernet_oam ports 1 remote_loopback start
Command: config ethernet_oam ports 1 remote_loopback start

Success.

```

```
DWS-3160-24PC:admin#
```

To configure the method of processing the received remote loopback command as “process” on port 1:

```
DWS-3160-24PC:admin# config ethernet_oam ports 1 received_remote_loopback
process
Command: config ethernet_oam ports 1 received_remote_loopback process

Success.

DWS-3160-24PC:admin#
```

51-2 show ethernet_oam ports

Description

This command is used to display Ethernet OAM information, including status, configuration, statistics, and event log, on specified ports.

The status information includes:

- OAM administration status: enabled or disabled.
- OAM operation status. It maybe the below value:
    - Disable: OAM is disabled on this port.
    - LinkFault: The link has detected a fault and is transmitting OAMPDUs with a link fault indication.
    - PassiveWait: The port is passive and is waiting to see if the peer device is OAM capable.
    - ActiveSendLocal: The port is active and is sending local information.
    - SendLocalAndRemote: The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer.
    - SendLocalAndRemoteOk: The local device agrees the OAM peer entity.
    - PeeringLocallyRejected: The local OAM entity rejects the remote peer OAM entity.
    - PeeringRemotelyRejected: The remote OAM entity rejects the local device.
    - Operational: The local OAM entity learns that both it and the remote OAM entity have accepted the peering.
    - NonOperHalfDuplex: Since Ethernet OAM functions are not designed to work completely over half-duplex port. This value indicates Ethernet OAM is enabled but the port is in half-duplex operation.
- OAM mode: passive or active.
- Maximum OAMPDU size: The largest OAMPDU that the OAM entity supports. OAM entities exchange maximum OAMPDU sizes and negotiate to use the smaller of the two maximum OAMPDU sizes between the peers.
- OAM configuration revision: The configuration revision of the OAM entity as reflected in the latest OAMPDU sent by the OAM entity. The config revision is used by OAM entities to indicate that configuration changes have occurred, which might require the peer OAM entity to re-evaluate whether OAM peering is allowed.
- OAM mode change.
- OAM Functions Supported: The OAM functions supported on this port. These functions include:

- Unidirectional: It indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (traffic flowing in one direction only).
- Loopback: It indicates that the OAM entity can initiate and respond to loopback commands.
- Link Monitoring: It indicates that the OAM entity can send and receive Event Notification OAMPDUs.
- Variable: It indicates that the OAM entity can send and receive variable requests to monitor the attribute value as described in the IEEE 802.3 Clause 30 MIB.

The event log displays Ethernet OAM event log information. The Switch can buffer 1000 event logs. The event log is different from sys-log as it provides more detailed information than sys-log. Each OAM event will be recorded in both OAM event log and syslog.

Format

show ethernet_oam ports {<portlist>} [status | configuration | statistics | event_log {index <value_list>}]

Parameters

<portlist> - (Optional) Specifies the range of ports to display.
status - Specifies to display the Ethernet OAM status.
configuration - Specifies to display the Ethernet OAM configuration.
statistics - Specifies to display Ethernet OAM statistics.
event_log - Specifies to display the Ethernet OAM event log information. **index** - (Optional) Specifies an index range to display. **<value_list>** - (Optional) Specifies an index range to display.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display Ethernet OAM statistics information for port 1:

```
DWS-3160-24PC:admin#show ethernet_oam ports 1 statistics
Command: show ethernet_oam ports 1 statistics

Port 1
-----------------------------------------------------------
  Information OAMPDU TX                 : 67
  Information OAMPDU RX                 : 0
  Unique Event Notification OAMPDU TX   : 0
  Unique Event Notification OAMPDU RX   : 0
  Duplicate Event Notification OAMPDU TX: 0
  Duplicate Event Notification OAMPDU RX: 0
  Loopback Control OAMPDU TX            : 0
  Loopback Control OAMPDU RX            : 0
  Variable Request OAMPDU TX            : 0
  Variable Request OAMPDU RX            : 0
  Variable Response OAMPDU TX           : 0
  Variable Response OAMPDU RX           : 0
  Organization Specific OAMPDUs TX      : 0
  Organization Specific OAMPDUs RX      : 0
  Unsupported OAMPDU TX                 : 0
  Unsupported OAMPDU RX                 : 0
  Frames Lost Due To OAM                : 0

DWS-3160-24PC:admin#
```

51-3 clear ethernet_oam ports

Description

This command is used to clear Ethernet OAM information.

Format

clear ethernet_oam ports [<portlist> | all] [event_log | statistics]

Parameters

<portlist> - Specifies a range of Ethernet OAM ports to be cleared.

all - Specifies to clear all Ethernet OAM ports.

event_log - Specifies to clear Ethernet OAM event log information.

statistics - Specifies to clear Ethernet OAM statistics.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear port 1 OAM statistics:

```
DWS-3160-24PC:admin# clear ethernet_oam ports 1 statistics
Command: clear ethernet_oam ports 1 statistics

Success.

DWS-3160-24PC:admin#
```

To clear port 1 OAM events:

```
DWS-3160-24PC:admin# clear ethernet_oam ports 1 event_log
Command: clear ethernet_oam ports 1 event_log

Success.

DWS-3160-24PC:admin#
```

Chapter 52 Peripherals Command List

show device_status
show environment
config temperature threshold {high <temperature -500-500> | low <temperature -500-500>}
config temperature [trap | log] state [enable | disable]

52-1 show device_status

Description

This command is used to display current status of power(s) and fan(s) on the Switch.

Format

show device_status

Parameters

None.

Restrictions

None.

Example

To display the device status:

```
DWS-3160-24PC:admin#show device_status
Command: show device_status

    Internal Power: Active
    External Power: Fail
    Right Fan     : OK

DWS-3160-24PC:admin#
```

52-2 show environment

Description

This command is used to display current status of power(s) and fan(s) on the system.

Format

show environment

Parameters

None.

Restrictions

None.

Example

To display the standalone device environment:

```
DWS-3160-24PC:admin#show environment
Command: show environment

Internal Power      : Active
External Power      : Fail
Right Fan 1         : Speed Low  (3000 RPM)
Right Fan 2         : Speed Low  (3000 RPM)
Right Fan 3         : Speed Low  (3000 RPM)
Right Fan 4         : Speed Low  (3000 RPM)
Current Temperature(Celsius) :   30
Fan High Temperature Threshold(Celsius)     :    40
Fan Low Temperature Threshold(Celsius)      :    35
High Warning Temperature Threshold(Celsius) :    79
Low Warning Temperature Threshold(Celsius)  :    11

DWS-3160-24PC:admin#
```

52-3 config temperature threshold

Description

This command is used to configure the warning threshold for high and low temperature. When the temperature is above the high threshold limit or below the low threshold limit, the Switch will send out alarm traps or automatically shut the Switch system down.

Format

config temperature threshold {high <temperature -500-500> | low <temperature -500-500>}

Parameters

threshold - Specifies the high and low threshold value.

high - (Optional) Specifies to configure the high threshold value. The high threshold must bigger than the low threshold.

<temperature -500-500> - Enter the high threshold temperature here. This value must be between -500 and 500.

low - (Optional) Specifies to configure the low threshold value.

<temperature -500-500> - Enter the low threshold temperature here. This value must be between -500 and 500.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the warning temperature threshold:

```
DWS-3160-24PC:admin# config temperature threshold high 80
Command: config temperature threshold high 80

Success.

DWS-3160-24PC:admin#
```

52-4 config temperature

Description

This command is used to configure the trap state for temperature warning event.

Format

config temperature [trap | log] state [enable | disable]

Parameters

trap state - Specifies the trap state for the warning temperature event.
 enable - Enable trap state for warning temperature event. The default state is enabled.
 disable - Disable trap state for warning temperature event.

log state - Specifies the log state for the warning temperature event.
 enable - Enable log state for warning temperature event. The default state is enabled.
 disable - Disable log state for warning temperature event.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the trap state for temperature warning event.

```
DWS-3160-24PC:admin#config temperature trap state enable
Command: config temperature trap state enable

Success.

DWS-3160-24PC:admin#
```

Chapter 53 Ping Command List

ping <ipaddr> {times <value 1-255> | timeout <sec 1-99>}

ping6 <ipv6addr> {times <value 1-255> | size <value 1-6000> | timeout <sec 1-99>}

53-1 ping

Description

This command is used to send out Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then echo or return the message. This is used to confirm connectivity between the Switch and the remote device.

Format

ping <ipaddr> {times <value 1-255> | timeout <sec 1-99>}

Parameters

<ipaddr> - Specifies the IP address of the host.

times - (Optional) The number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0, indicating infinity. Press the "CTRL+C" to break the ping test.

<value 1-255> - Enter the number of individual ICMP echo messages to be sent here. This value must be between 1 and 255.

timeout - (Optional) Defines 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.

<sec 1-99> - Enter the time-out period here. This value must be between 1 and 99 seconds.

Restrictions

None.

Example

To send ICMP echo message to “10.51.17.1” for 4 times:

```
DWS-3160-24PC:admin# ping 10.51.17.1 times 4
Command: ping 10.51.17.1 times 4

Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms

Ping Statistics for 10.51.17.1
Packets: Sent =4, Received =4, Lost =0

DWS-3160-24PC:admin#
```

53-2 ping6

Description

This command is used to send out IPv6 Internet Control Message Protocol (ICMP) echo messages to a remote IPv6 address. The remote IPv6 address will then echo or return the message. This is used to confirm the IPv6 connectivity between the Switch and the remote device.

Format

ping6 <ipv6addr> {times <value 1-255> | size <value 1-6000> | timeout <sec 1-99>}

Parameters

<ipv6addr> - Enter the IPv6 address here.

times - (Optional) The number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0, indicating infinity. Press the "CTRL+C" to break the ping test.

<value 1-255> - Enter the number of individual ICMP echo messages to be sent here. This value must be between 1 and 255.

size - (Optional) Size of the test packet.

<value 1-6000> - Enter the size of the test packet here. This value must be between 1 and 6000.

timeout - (Optional) Defines the time-out period while waiting for a response from the remote device. A value of 1 to 10 seconds can be specified. The default is 1 second.

<sec 1-99> - Enter the time-out period here. This value must be between 1 and 99 seconds.

Restrictions

None.

Example

To send ICMP echo message to “3000::1” for 4 times:

```
DWS-3160-24PC:admin# ping6 3000::1 times 4
Command: ping6 3000::1 times 4

Reply from 3000::1, bytes=200, time<10ms
Reply from 3000::1, bytes=200, time<10ms
Reply from 3000::1, bytes=200, time<10ms
Reply from 3000::1, bytes=200, time<10ms

Ping Statistics for 3000::1
Packets: Sent =4, Received =4, Lost =0

DWS-3160-24PC:admin#
```

Chapter 54 Port Security Command List

config port_security system max_learning_addr [<max_lock_no 1-3072> | no_limit]

config port_security ports [<portlist> | all] [{admin_state [enable | disable] | max_learning_addr <max_lock_no 0-3072> | lock_address_mode [permanent | deleteontimeout | deleteonreset]}(1)| {vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3072> | no_limit]}(1)]

config port_security vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3072> | no_limit]

delete port_security_entry [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>

clear port_security_entry {ports [<portlist> | all] {[vlan <vlan_name 32> | vlanid <vidlist>]}}

show port_security_entry {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}

show port_security {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}

enable port_security trap_log

disable port_security trap_log

54-1 config port_security system max_learning_addr

Description

This command is used to configure the maximum number of port security entries that can be authorized system wide. There are four levels of limitations on the learned entry number; for the entire system, for a port, for a VLAN, and for a specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded. The setting for system level maximum learned users must be greater than the total of maximum learned users allowed on all ports.

Format

config port_security system max_learning_addr [<max_lock_no 1-3072> | no_limit]

Parameters

max_learning_addr - Specifies the maximum number of port security entries that can be learned by the system. If the setting is smaller than the number of current learned entries on all enabled ports, the command will be rejected.

<max_lock_no 1-3072> - Enter the maximum learning address value here. This value must be between 1 and 3072.

no_limit - No limitation on the number of port security entries that can be learned by the system. By default, the number is set to no_limit.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the maximum number of port security entries on the Switch to be 256:

```
DWS-3160-24PC:admin# config port_security system max_learning_addr 256
Command: config port_security system max_learning_addr 256

Success.

DWS-3160-24PC:admin#
```

54-2 config port_security ports

Description

This command is used to configure the maximum number of addresses that can be learned and the lock address mode. There are four levels that limit the number of learned entries; the entire system, a port, a VLAN, and a specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded.

Format

config port_security ports [<portlist> | all] [{admin_state [enable | disable] | max_learning_addr <max_lock_no 0-3072> | lock_address_mode [permanent | deleteontimeout | deleteonreset]} (1)| {vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3072> | no_limit]}(1)]

Parameters

ports - Specifies the range of ports to be configured.
<portlist> - Enter the list of port used for this configuration here.
all - Specifies that all ports will be configured.

admin_state - (Optional) Specifies the state of the port security function on the port.
enable - Specifies to enable the port security function on the port.
disable - Specifies to disable the port security function on the port. By default, the setting is disabled.

max_learning_addr - (Optional) Specifies the maximum number of port security entries that can be learned on this port. If the value is set to 0, it means that no user can be authorized by the port security function on this port. If the setting is smaller than the number of current learned entries on the port, the command will be rejected. The default value is 32.
<max_lock_no 0-3072> - Enter the maximum number of port security entries that can be learned here. This value must be between 0 and 3072.

lock_address_mode - (Optional) Indicates the lock address mode. The default mode is deleteonreset.
permanent - The address will never be deleted unless the user removes it manually, the VLAN of the entry is removed, the port is removed from the VLAN, or port security is disabled on the port where the address resides.
deleteontimeout - This entry will be removed if the entry is idle for the specified aging time.
deleteonreset - This address will be removed if the Switch is reset or rebooted. Events that cause permanent entries to be deleted also apply to the deleteonreset entries.

vlan - (Optional) Specifies the VLAN name used here.
<vlan_name 32> - Enter the VLAN name used here. This name can be up to 32 characters long.

vlanid - (Optional) Specifies the VLAN ID used here.
<vidlist> - Enter the VLAN ID used here.

max_learning_addr - (Optional) Specifies the maximum learning address value.
<max_lock_no 0-3072> - Enter the maximum learning address value here. This value must be between 0 and 3072.
no_limit - Specifies that the maximum learning address value will be set to no limit.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the port-based port security setting so that the maximum number of port security entries is restricted to 10, and the lock address mode is set to permanent on port 6:

```
DWS-3160-24PC:admin#config port_security ports 6 admin_state enable
max_learning_addr 10 lock_address_mode permanent
Command: config port_security ports 6 admin_state enable max_learning_addr 10
lock_address_mode permanent

Success.

DWS-3160-24PC:admin#
```

54-3 config port_security vlan

Description

This command is used to configure the maximum number of port security entries that can be learned on a specific VLAN. There are four levels that limit the number of learned entries; the entire system, a port, a VLAN, and a specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded.

Format

config port_security vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3072> | no_limit]

Parameters

vlan - Specifies the VLAN by name.

<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

vlanid - Specifies a list of VLANs by VLAN ID.

<vidlist> - Enter the VLAN ID list here.

max_learning_addr - Specifies the maximum number of port security entries that can be learned by this VLAN. If this parameter is set to 0, it means that no user can be authorized on this VLAN. If the setting is lower than the number of current learned entries on the VLAN, the command will be rejected. The default value is “no_limit”

<max_lock_no 0-3072> - Enter the maximum number of port security entries that can be learned here. This value must be between 0 and 3072.

no_limit - No limitation on the number of port security entries that can be learned by a specific VLAN.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the maximum number of VLAN-based port security entries on VLAN 1 to be 64:

```
DWS-3160-24PC:admin# config port_security vlan vlanid 1 max_learning_addr 64
Command: config port_security vlan vlanid 1 max_learning_addr 64

Success.

DWS-3160-24PC:admin#
```

54-4 delete port_security_entry

Description

This command is used to delete a port security entry.

Format

delete port_security_entry [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>

Parameters

vlan - Specifies the VLAN by VLAN name. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specifies the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID list here. This value must be between 1 and 4094.
mac_address - Specifies the MAC address of the entry. **<macaddr>** - Enter the MAC address used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the port security entry with a MAC address of 00-00-00-00-00-01 on VLAN 1:

```
DWS-3160-24PC:admin# delete port_security_entry vlanid 1 mac_address 00-00-00-
00-00-01
Command: delete port_security_entry vlanid 1 mac_address 00-00-00-00-00-01

Success.

DWS-3160-24PC:admin#
```

54-5 clear port_security_entry

Description

This command is used to clear the MAC entries learned by the port security function.

Format

clear port_security_entry {ports [<portlist> | all] {[vlan <vlan_name 32> | vlanid <vidlist>]}}

Parameters

ports - (Optional) Specifies the range of ports to be configured.
<portlist> - The port security entries learned on the specified port will be cleared.
all - All the port security entries learned by the system will be cleared.

vlan - (Optional) The port security entries learned on the specified VLANs will be cleared.
<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

vlanid - (Optional) Specifies a list of VLANs by VLAN ID.
<vidlist> - Enter the VLAN ID list here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear the port security entries on port 6:

```
DWS-3160-24PC:admin# clear port_security_entry ports 6
Command: clear port_security_entry ports 6

Success.

DWS-3160-24PC:admin#
```

54-6 show port_security_entry

Description

This command is used to display the port security entries. If more than one parameter is selected, only the entries matching all the selected parameters will be displayed. If the user specifies ports and VLANs (either the VLAN name or VLAN ID list), only the entries matching all the parameters will be displayed.

Format

show port_security_entry {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}

Parameters

ports - (Optional) Specifies the range of ports that will display the port security entries. While this parameter is null, to display the entries on all of the ports.
<portlist> - Enter the list of port used for this configuration here.

vlan - (Optional) Specifies the name of the VLAN that the port security settings will be displayed for.
<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

vlanid - (Optional) Specifies the ID of the VLAN that the port security entries will be displayed for.
<vidlist> - Enter the VLAN ID list here.

Restrictions

None.

Example

To display all the port security entries:

```
DWS-3160-24PC:admin#show port_security_entry
Command: show port_security_entry

 MAC Address        VID   Port   Lock Mode
 -----------------  ----  -----  ---------------
 00-11-22-33-32-32  1     23     Permanent
 00-22-B0-3C-43-C0  1     23     Permanent
 00-22-B0-3C-DD-C0  1     2      Permanent
 02-23-7D-BC-08-44  1     1      Permanent
 F0-7D-68-78-92-A4  1     1      Permanent

 The Total Entry Number: 5

DWS-3160-24PC:admin#show port_security_entry ports
Command: show port_security_entry ports

 MAC Address        VID   Port   Lock Mode
 -----------------  ----  -----  ---------------
 00-11-22-33-32-32  1     23     Permanent
 00-22-B0-3C-43-C0  1     23     Permanent
 00-22-B0-3C-DD-C0  1     2      Permanent
 00-23-7D-BC-2E-18  1     1      Permanent
 02-23-7D-BC-08-44  1     1      Permanent
 F0-7D-68-78-92-A4  1     1      Permanent

 The Total Entry Number: 6

DWS-3160-24PC:admin#
```

54-7 show port_security

Description

This command is used to display the port security related information, including state, maximum learned addresses and lock address mode on a port and/or on a VLAN.

If both ports and vlanid (or vlan_name) are specified, configurations matching any of these parameters will be displayed.

Format

show port_security {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}

Parameters

ports - (Optional) Specifies the range of ports that will display their configuration. While this parameter is null, to display the entries on all of the ports.
<portlist> - Enter the list of port used for this configuration here.

vlan - (Optional) Specifies the name of the VLAN that will display its configuration.
<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

vlanid - (Optional) Specifies the ID of the VLAN that will display its configuration.
<vidlist> - Enter the VLAN ID list here.

Restrictions

None.

Example

To display the global configuration of port security:

```
DWS-3160-24PC:admin#show port_security
Command: show port_security

 Port Security Trap/Log        : Disabled
 System Maximum Address        : 256

 VLAN Configuration (Only VLANs with limitation are displayed)
 VID   VLAN Name                        Max. Learning Addr.
 ----  -------------------------------  ------------------
 1     default                          64

DWS-3160-24PC:admin#
```

54-8 enable port_security trap_log

Description

This command is used to enable the port security trap/log. When the port security trap is enabled, if there is a new MAC address that violates the pre-defined port security configuration, a trap will be sent out with the MAC address, port and other relevant information being logged.

Format

enable port_security trap_log

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the port security trap and save the log:

```
DWS-3160-24PC:admin# enable port_security trap_log
Command: enable port_security trap_log

Success.

DWS-3160-24PC:admin#
```

54-9 disable port_security trap_log

Description

This command is used to disable the port security trap/log. If the port security trap is disabled, no trap will be sent out for a MAC violation.

Format

disable port_security trap_log

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the port security trap/log:

```
DWS-3160-24PC:admin# disable port_security trap_log
Command: disable port_security trap_log

Success.

DWS-3160-24PC:admin#
```

Chapter 55 Power over Ethernet (PoE) Command List

config poe system {power_limit <value 37-740> | power_disconnect_method [deny_next_port | deny_low_priority_port] | legacy_pd [enable | disable]}

config poe ports [all | <portlist>] { state [enable | disable]| [time_range <range_name 32> | clear_time_range]| priority [critical | high | low] | power_limit [class_0 | class_1 | class_2 | class_3 | user_define <value 1000-35000>]}

show poe system

show poe ports {<portlist>}

55-1 config poe system

Description

This command is used to configure the PoE system-wise function.

Format

config poe system {power_limit <value 37-740> | power_disconnect_method [deny_next_port | deny_low_priority_port] | legacy_pd [enable | disable]}

Parameters

power_limit - (Optional) Configure the power budget of PoE system. The range of value which can be specified is determined by the system. Normally, the minimum setting is 37 W and the maximum setting is 740 W. The actual range will depend on power supply capability.

<value 37-740> - Enter the power limit value here. This value must be between 37 and 740.

power_disconnect_method - (Optional) Configure the disconnection method that will be used when the power budget is running out. When the system attempts to supply power to a new port, if the power budget is insufficient to do this, PoE controller will initiate port disconnection procedure to prevent overloading the power supply. The controller uses one of the following two ways to perform the disconnection procedure.

deny_next_port - The port with max port number will be denied regardless of its priority. Note that if the disconnect method is set to deny_next_port, then the power provision will not utilize the system’s maximum power. There is a 19W safe margin. That is, when the system has only 19W remaining, this power cannot be utilized.

deny_low_priority_port - If there are ports that have been supplied power that have a priority lower than the new port, the port with the lowest priority will be disconnected. This process will stop until enough power is released for the new port. Note that if the disconnect method is set to deny low priority port, then the power provision can utilize the system’s maximum power.

legacy_pd - Configure legacy PDs detection status, enable for support, if set to disable, can’t detect legacy PDs signal.

enable - Specifies that the legacy PDs detection status will be enabled.

disable - Specifies that the legacy PDs detection status will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To config PoE system-wise was setting:

```
DWS-3160-24PC:admin#config poe system power_limit 250 power_disconnect_method
deny_low_priority_port
Command: config poe system power_limit 250 power_disconnect_method
deny_low_priority_port

Success.

DWS-3160-24PC:admin#
```

55-2 config poe ports

Description

This command is used to configure the PoE port settings.

Based on 802.3af, there are 5 kinds of PD classes, class 0, class 1, class 2, and class 3. The power consumption ranges for them are 0.44~12.95W, 0.44~3.84W, 3.84~6.49W, 6.49~12.95W, and 12.95~ 29.5W, respectively.

The five pre-defined settings are for users' convenience: The following is the power limit applied to the port for these four classes. For each class, the power limit is a little more than the power consumption range for the class. This takes the factor of the power loss on cable into account.

Thus, the following are the typical values defined by the chip vendor.

- Class 0: 15400mW
- Class 1: 4000mW
- Class 2: 7000mW
- Class 3: 15400mW

Other than these four pre-defined settings, users can directly specify any value that the chip supports. Normally, the minimum setting is 1000mW, and the maximum setting is 15400mW for 802.3af and >=35000mW for 802.3at.

Format

config poe ports [all | <portlist>] { state [enable | disable] | [time_range <range_name 32> | clear_time_range] | priority [critical | high | low] | power_limit [class_0 | class_1 | class_2 | class_3 | user_define <value 1000-35000>]}

Parameters

ports - Specified the list of ports whose setting is under configuration.
all - Specifies that all the ports will be included in this configuration.
<portlist> - Enter the list of port used for this configuration here.

state - (Optional) When the state is set to disable, power will not be supplied to the powered device connected to this port.
enable - Specifies that state will be enabled.
disable - Specifies that state will be disabled.

time_range - (Optional) Specifies the time range that applies to the port of the POE. If time range is configured, the power can only be supplied during the period specified by time range.
<range_name 32> - Enter the time range name here. This name can be up to 32 characters

long.

clear_time_range - (Optional) Remove the time range.

priority - (Optional) Port priority determines the priority the system attempts to supply the power to port. There are three levels of priority that can be selected, critical, high, and low. When multiple ports happen to have the same level of priority, the port ID will be used to determine the priority. The lower port ID has higher priority. The setting of priority will affect the ordering of supplying power. Whether the disconnect method is set to deny_low_priority_port, priority of port will be used by the system to manage to supply power to ports.

critical - Specifies that the priority will be set to critical.

high - Specifies that the priority will be set to high.

low - Specifies that the priority will be set to low.

power_limit - (Optional) Configure the per-port power limit. If a port exceeds its power limit, it will be shut down.

class_0 - Specifies that the power limit will be set to class 0.

class_1 - Specifies that the power limit will be set to class 1.

class_2 - Specifies that the power limit will be set to class 2.

class_3 - Specifies that the power limit will be set to class 3.

user_define - (Optional) Specifies that a user defined per-port power limit will be used.

<value 1000-35000> - Enter the user defined per-port power limit here. This value must be between 1000 and 35000.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure PoE port:

```
DWS-3160-24PC:admin#config poe ports 1-4 state enable priority critical
power_limit class_1
Command: config poe ports 1-4 state enable priority critical power_limit
class_1


 Power limit has been set to 4000 (Class 1 PD upper power limit 3.84W + power
loss on cable)
Success.


DWS-3160-24PC:admin#config poe ports 5 state enable priority critical
power_limit user_define 1000
Command: config poe ports 5 state enable priority critical power_limit
user_define 1000


 Power limit has been set to 1000 (User-define power limit should be greater
than 1.18*PD_Request_Power, consider cable loss)
Success.


DWS-3160-24PC:admin#
```

55-3 show poe system

Description

This command is used to display the configuration and actual values of the whole PoE system.

Format

show poe system

Parameters

None.

Restrictions

None.

Example

To display the PoE system:

```
DWS-3160-24PC:admin#show poe system
Command: show poe system

PoE System Information
---------------------------------------------------
Power Limit                 : 250(Watts)
Power Consumption           : 0(Watts)
Power Remained              : 250(Watts)
Power Disconnection Method : Deny Low Priority Port
Detection Legacy PD         : Disabled

If Power Disconnection Method is set to deny next port, then the system can not
utilize out of its maximum power capacity. The maximum unused watt is 19W.

DWS-3160-24PC:admin#
```

55-4 show poe ports

Description

This command is used to display the configuration and actual values of the PoE port(s).

Format

show poe ports {<portlist>}

Parameters

<portlist> - (Optional) Specified a list of ports to be displayed.
If no parameter specified, the system will display the status for all ports.

Restrictions

None.

Example

To display PoE information of ports 1 to 6:

```
DWS-3160-24PC:admin#show poe ports 1-6
Command: show poe ports 1-6

Port   State     Priority  Power Limit(mW)     Time Range
       Class     Power(mW) Voltage(decivolt)   Current(mA)
       Status
================================================================================
1      Enabled   Critical  4000 (Class 1)
       0         0         0                   0
       OFF  : Interim state during line detection
2      Enabled   Critical  4000 (Class 1)
       3         0         0                   0
       OFF  : Overload state according to 802.3af
3      Enabled   Critical  4000 (Class 1)
       0         0         0                   0
       OFF  : Interim state during line detection
4      Enabled   Critical  4000 (Class 1)
       0         0         0                   0
       OFF  : Interim state during line detection
5      Enabled   Critical  1000 (User-defined)
       0         0         0                   0
       OFF  : Interim state during line detection
6      Enabled   Low       15400(Class 0)
       0         0         0                   0
       OFF  : Interim state during line detection
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Chapter 56 Power Saving Command List

config power_saving {state [enable | disable] | length_detection [enable | disable]} (1)
show power_saving

56-1 config power_saving

Description

This command is used to configure the power saving parameters found on this Switch. By default, the power saving mode is enabled. The power saving function applies to the port with copper media. Power is saved by the following mechanisms.

When the port has no link partner, the port automatically turns off and wakes up once a second to send a single link pulse. While the port is turned off, a simple receive energy-detect circuit is continuously monitoring energy on the cable. At the moment when energy is detected, the port turns on fully as IEEE specification’s requirements. The power saving function is performed while no link is detected and it will not affect the port capabilities while it’s link up.

When the port is link up, for shorter cable, the power consumption can be reduced by lowering the signal amplitude since the signal attenuation is proportional to the cable length. The port will adjust the power based on cable length and still maintain error free applications from both side of the link. This mechanism will only be supported when hardware support cable diagnostics function.

Format

config power_saving {state [enable | disable] | length_detection [enable | disable]} (1)

Parameters

state - (Optional) Enable or disable the power saving function. The default state is enabled. **enable** - Specifies that the power saving function will be enabled. **disable** - Specifies that the power saving function will be disabled.
length_detection - (Optional) Enable or disable the length detection function. The default state is disabled. **enable** - Specifies that the length detection function will be enabled. **disable** - Specifies that the length detection function will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

Te enable the power saving function:

```
DWS-3160-24PC:admin# config power_saving state enable
Command: config power_saving state enable

Success.

DWS-3160-24PC:admin#
```

56-2 show power_saving

Description

This command is used to display the current state of power saving.

Format

show power_saving

Parameters

None.

Restrictions

None.

Example

This example display the power saving function setting:

```
DWS-3160-24PC:admin#show power_saving
Command: show power_saving

Power Saving State: Enabled

Length Detection State: Disabled

DWS-3160-24PC:admin#
```

Chapter 57 Protocol VLAN Command List

create dot1v_protocol_group group_id <id> {group_name <name 32>}
config dot1v_protocol_group [group_id <id> | group_name <name 32>] [add protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value> | delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>]
delete dot1v_protocol_group [group_id <id> | group_name <name 32> | all]
show dot1v_protocol_group {[group_id <id> | group_name <name 32>]}
config port dot1v ports [<portlist> | all] [add protocol_group [group_id <id> | group_name <name 32>] [vlan <vlan_name 32> | vlanid <id>] {priority <value 0-7>} | delete protocol_group [group_id <id> | all]]
show port dot1v {ports <portlist>}

57-1 create dot1v_protocol_group

Description

This command is used to create a protocol group for the protocol VLAN function.

Format

create dot1v_protocol_group group_id <id> {group_name <name 32>}

Parameters

group_id - The ID of protocol group which is used to identify a set of protocols **<id>** - Enter the group ID used here.
group_name - (Optional) The name of the protocol group. The maximum length is 32 chars. If group name is not specified, the group name will be automatically generated in accordance with ProtocolGroup+group_id. For example, the auto-generated name for group id 2 is ProtocolGroup2. If the auto-generated name is in conflict with an existing group, an alternative name will be used in accordance with ProtocolGroup+group_id+ALT+num. The value for num starts with 1. If it is still in conflict, then previous number will be used instead. **<name 32> -** Enter the group name here. This name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a protocol group:

```
DWS-3160-24PC:admin# create dot1v_protocol_group group_id 10 group_name
General_Group
Command: create dot1v_protocol_group group_id 10 group_name General_Group

Success.

DWS-3160-24PC:admin#
```

57-2 config dot1v_protocol_group add protocol

Description

This command is used to add a protocol to a protocol group. The selection of a protocol can be a pre-defined protocol type or a user defined protocol.

Format

config dot1v_protocol_group [group_id <id> | group_name <name 32>] [add protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value> | delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>]

Parameters

group_id - The ID of the protocol group which is used to identify a set of protocols. **<id>** - Enter the group ID used here.
group_name - The name of the protocol group. **<name 32>** - Enter the group name here. This name can be up to 32 characters long.
add - Specifies that the protocol will be added to the specified group.
delete - Specifies that the protocol will be removed from the specified group.
protocol - The protocol value is used to identify a protocol of the frame type specified. **ethernet_2** - Specifies that the Ethernet 2 protocol will be used. **ieee802.3_snap** - Specifies that the IEEE 802.3 Snap protocol will be used. **ieee802.3_llc** - Specifies that the IEEE 802.3 LLC protocol will be used. **<protocol_value>** - Enter the protocol value here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a protocol IPv6 to protocol group 100:

```
DWS-3160-24PC:admin#config dot1v_protocol_group group_id 10 add protocol
ethernet_2 86DD
Command: config dot1v_protocol_group group_id 10 add protocol ethernet_2 86DD

Success.

DWS-3160-24PC:admin#
```

57-3 delete dot1v_protocol_group

Description

This command is used to delete a protocol group.

Format

delete dot1v_protocol_group [group_id <id> | group_name <name 32> | all]

Parameters

group_id - Specifies the group ID to be deleted.
<id> - Enter the group ID used here.

group_name - Specifies the name of the group to be deleted.
<name 32> - Enter the group name here. This name can be up to 32 characters long.

all - Specifies that all the protocol group will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the protocol group 100:

```
DWS-3160-24PC:admin# delete dot1v_protocol_group group_id 100
Command: delete dot1v_protocol_group group_id 100

Success.

DWS-3160-24PC:admin#
```

57-4 show dot1v_protocol_group

Description

This command is used to display the protocols defined in a protocol group.

Format

show dot1v_protocol_group {[group_id <id> | group_name <name 32>]}

Parameters

group_id - (Optional) Specifies the ID of the group to be displayed.
<id> - Enter the group ID used here.

group_name - (Optional) Specifies the name of the protocol group to be displayed.
<name 32> - Enter the group name here. This name can be up to 32 characters long.

If no group ID is not specified, all the configured protocol groups will be displayed.

Restrictions

None.

Example

To display the protocol group ID 100:

```
DWS-3160-24PC:admin#show dot1v_protocol_group group_id 10
Command: show dot1v_protocol_group group_id 10

Protocol Group ID Protocol Group Name              Frame Type     Protocol
Value
----------------- -------------------------------- -------------- -------------
10                General_Group                    EthernetII     86DD

Total Entries: 1

DWS-3160-24PC:admin#
```

57-5 config port dot1v

Description

This command is used to assign the VLAN for untagged packets ingress from the port list based on the protocol group configured. When priority is not specified in the command, the port default priority will be the priority for those untagged packets classified by the protocol vlan.

Format

config port dot1v ports [<portlist> | all] [add protocol_group [group_id <id> | group_name <name 32>] [vlan <vlan_name 32> | vlanid <id>] {priority <value 0-7>} | delete protocol_group [group_id <id> | all]]

Parameters

<portlist> - Enter a list of ports used for the configuration here.
all - Specifies that all the ports will be used for this configuration.

add - Specifies that the group specified will be added.

protocol_group - Specifies that parameters for the group will follow.

group_id - Specifies the group ID of the protocol group.
    <id> - Enter the group ID used here.

group_name - Specifies the name of the protocol group.
    <name 32> - Enter the name of the group used here. This name can be up to 32 characters long.

vlan - The VLAN that is to be associated with this protocol group on this port.
    <vlan_name 32> - Enter the name of the VLAN here. This name can be up to 32 characters long.

vlanid - Specifies the VLAN ID.
    <id> - Enter the VLAN ID used here.

priority - (Optional) Specifies the priority to be associated with the packet which has been classified to the specified VLAN by the protocol.
    <value 0-7> - Enter the priority value here. This value must be between 0 and 7.

delete - Specifies that the group specified will be deleted.

protocol_group - Specifies that parameters for the group will follow.

group_id - Specifies the group ID of the protocol group.
    <id> - Enter the group ID used here.
    all - Specifies that all the groups will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

The example is to assign VLAN marketing-1 for untagged ipv6 packet ingress from port 3.

To configure the group ID 100 on port 3 to be associated with VLAN marketing-1:

```
DWS-3160-24PC:admin#config port dot1v ports 3 add protocol_group group_id 10
vlan marketing-1
Command: config port dot1v ports 3 add protocol_group group_id 10 vlan
marketing-1

Success.

DWS-3160-24PC:admin#
```

57-6 show port dot1v

Description

This command is used to display the VLAN associated with untagged packet ingressed from a port based on the protocol group.

Format

show port dot1v {ports <portlist>}

Parameters

ports - (Optional) Specifies a range of ports to be displayed. **<portlist>** - Enter a list of ports used for the configuration here.
If not port is specified, information for all ports will be displayed.

Restrictions

None.

Example

The example display the protocol VLAN information for port 3:

```
DWS-3160-24PC:admin#show port dot1v ports 3
Command: show port dot1v ports 3

 Port: 3
 Protocol Group ID     VLAN Name                            Protocol Priority
 -------------------   ---------------------------------   -----------------
 10                    marketing-1                          -

Total Entries: 1

DWS-3160-24PC:admin#
```

Chapter 58 QinQ Command List

enable qinq

disable qinq

config qinq inner_tpid <hex 0x1-0xffff>

config qinq ports [<portlist> | all] {role [uni | nni] | missdrop [enable | disable] | outer_tpid <hex 0x1-0xffff> | add_inner_tag [<hex 0x1-0xffff> | disable]}

show qinq

show qinq inner_tpid

show qinq ports {<portlist>}

create vlan_translation ports [<portlist> | all] [add cvid <vidlist> | replace cvid <vlanid 1-4094>] svid <vlanid 1-4094> {priority <priority 0-7>}

delete vlan_translation ports [<portlist> | all] {cvid <vidlist>}

show vlan_translation {[ports <portlist> | cvid <vidlist>]}

58-1 enable qinq

Description

This command is used to enable QinQ. When QinQ is enabled, all network port roles will be NNI ports and outer TPID will be set to 0x88A8; all existing static VLANs will run as S-VLAN; all dynamic learned Layer 2 address will be cleared; all dynamic registered VLAN entries will be cleared; and GVRP will be disabled.

To run GVRP on the Switch, the administrator should enable GVRP manually. In QinQ mode, GVRP protocol will employ reserve address 01-80-C2-00-00-0D.

Format

enable qinq

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable QinQ:

```
DWS-3160-24PC:admin# enable qinq
Command: enable qinq

Success.

DWS-3160-24PC:admin#
```

58-2 disable qinq

Description

This command is used to disable the QinQ. When QinQ is disabled, all dynamic learned Layer 2 addresses will be cleared, all dynamic registered VLAN entries will be cleared, and GVRP will be disabled.

To run GVRP on the Switch, the administrator should enable GVRP manually.

Format

disable qinq

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable QinQ:

```
DWS-3160-24PC:admin# disable qinq
Command: disable qinq

Success.

DWS-3160-24PC:admin#
```

58-3 config qinq inner_tpid

Description

The command is used to configure the inner TPID of the system. The inner TPID is used to decide if the ingress packet is c-tagged. Inner tag TPID is per system configurable.

Format

config qinq inner_tpid <hex 0x1-0xffff>

Parameters

inner_tpid - Specifies the inner-TPID of the system.
<hex 0x1-0xffff> - Enter the inner-TPID of the system here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the inner TPID in the system to 0x9100:

```
DWS-3160-24PC:admin# config qinq inner_tpid 0x9100
Command: config qinq inner_tpid 0x9100

Success.

DWS-3160-24PC:admin#
```

58-4 config qinq ports

Description

This command is used to configure the QinQ port's parameters.

Format

config qinq ports [<portlist> | all] {role [uni | nni] | missdrop [enable | disable] | outer_tpid <hex 0x1-0xffff> | add_inner_tag [<hex 0x1-0xffff> | disable]}

Parameters

ports - Specifies a range of ports to configure.
- **<portlist>** - Enter the list of ports to be configured here.
- **all** - Specifies that all the ports will be used for the configuration.

role - (Optional) Specifies the port role in QinQ mode.
- **uni** - Specifies that the port is connecting to the customer network.
- **nni** - Specifies that the port is connecting to the service provider network.

missdrop - (Optional) Specifies the state of the miss drop of ports option.
- **enable** - Specifies that the miss drop of ports option will be enabled.
- **disable** - Specifies that the miss drop of ports option will be disabled.

outer_tpid - (Optional) Specifies the outer-TPID of a port.
- **<hex 0x1-0xffff>** - Enter the outer-TPID value used here.

add_inner_tag - (Optional) Specifies to add an inner tag for ingress untagged packets. If set, the inner tag will be added for the ingress untagged packets and therefore the packets that egress to the NNI port will be double tagged. If disable, only the s-tag will be added for ingress untagged packets.
- **<hex 0x1-0xffff>** - Enter the inner tag value used here.
- **disable** - Specifies that the add inner tag option will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure port list 1-4 as NNI port and set the TPID to 0x88A8:

```
DWS-3160-24PC:admin# config qinq ports 1-4 role nni outer_tpid 0x88A8
Command: config qinq ports 1-4 role nni outer_tpid 0x88A8

Success.

DWS-3160-24PC:admin#
```

58-5 show qinq

Description

This command is used to display the global QinQ status.

Format

show qinq

Parameters

None.

Restrictions

None.

Example

To display the global QinQ status:

```
DWS-3160-24PC:admin# show qinq
Command: show qinq

 QinQ Status : Enabled

DWS-3160-24PC:admin#
```

58-6 show qinq inner_tpid

Description

This command is used to display the inner-TPID of a system.

Format

show qinq inner_tpid

Parameters

None.

Restrictions

None.

Example

To display the inner-TPID of a system:

```
DWS-3160-24PC:admin# show qinq inner_tpid
Command: show qinq inner_tpid

 Inner TPID: 0x9100

DWS-3160-24PC:admin#
```

58-7 show qinq ports

Description

This command is used to display the QinQ configuration of the ports.

Format

show qinq ports {<portlist>}

Parameters

ports - Specifies a list of ports to be displayed.

<portlist> - (Optional) Enter the list of ports to be displayed here.

Restrictions

None.

Example

To display the QinQ mode for ports 1-2:

```
DWS-3160-24PC:admin#show qinq ports 1-2
Command: show qinq ports 1-2

Port ID:    1
---------------------------------------------------------
  Role:                     NNI
  Miss Drop:                Disabled
  Outer Tpid:               0x88a8
  Add Inner Tag:            Disabled

Port ID:    2
---------------------------------------------------------
  Role:                     NNI
  Miss Drop:                Disabled
  Outer Tpid:               0x88a8
  Add Inner Tag:            Disabled

DWS-3160-24PC:admin#
```

58-8 create vlan_translation ports

Description

This command is used to create a VLAN translation rule. This setting will not be effective when the QinQ mode is disabled.

This configuration is only effective for a UNI port. At UNI port, the ingress C-VLAN tagged packets will be translated to S-VLAN tagged packets by adding or replacing according the configured rule. The S-VLAN Tag of egress packets at this port will be recovered to C-VLAN Tag or stripped.

Format

create vlan_translation ports [<portlist> | all] [add cvid <vidlist> | replace cvid <vlanid 1-4094>] svid <vlanid 1-4094> {priority <priority 0-7>}

Parameters

ports - Specifies a list of ports to be configured. **<portlist>** - Enter the list of ports to be configured here. **all** - Specifies that all the ports will be used for the configuration.
add - Specifies to add an S-Tag to the packet. **cvid** - Specifies the customer VLAN ID used. **<vidlist>** - Enter the customer VLAN ID used here.
replace - Specifies to replace the C-Tag with the S-Tag. **cvid** - Specifies the customer VLAN ID used. **<vlanid 1-4094>** - Enter the customer VLAN ID used here. **svid** - Specifies the service provider VLAN ID used. **<vlanid 1-4094>** - Enter the service provider VLAN ID used here.
priority - (Optional) Specifies to assign an 802.1p priority to the S-Tag. If the priority is not specified, a 802.1p priority of the S-Tag will be assigned by default. **<priority 0-7>** - Enter the 802.1p S-Tag priority value here. This value must be between 0 and 7.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To replace the C-Tag in which the CVID is 2, with the S-Tag and the S-VID is 3 at UNI Port 1:

```
DWS-3160-24PC:admin#create vlan_translation ports 1 replace cvid 2 svid 3
Command: create vlan_translation ports 1 replace cvid 2 svid 3

Success.

DWS-3160-24PC:admin#
```

To add S-Tag, when the S-VID is 2, to a packet in which the CVID is 3 at UNI Port 1:

```
DWS-3160-24PC:admin#create vlan_translation ports 1 add cvid 3 svid 2
Command: create vlan_translation ports 1 add cvid 3 svid 2

Success.

DWS-3160-24PC:admin#
```

58-9 delete vlan_translation ports

Description

This command is used to delete translation relationships between the C-VLAN and the S-VLAN.

Format

delete vlan_translation ports [<portlist> | all] {cvid <vidlist>}

Parameters

ports - Specifies a list of ports to be configured.
<portlist> - Enter the list of ports to be configured here.
all - Specifies that all the ports will be used for the configuration.

cvid - (Optional) Specifies the rules for the specified CVIDs. If the CVID is not specified, all rules configured for the port will be deleted.
<vidlist> - Enter the CVID value here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a VLAN translation rule on ports 1-4:

```
DWS-3160-24PC:admin# delete vlan_translation ports 1-4
Command: delete vlan_translation ports 1-4

Success.

DWS-3160-24PC:admin#
```

58-10 show vlan_translation

Description

This command is used to display the existing C-VLAN-based VLAN translation rules.

Format

show vlan_translation {[ports <portlist> | cvid <vidlist>]}

Parameters

ports – (Optional) Specifies a list of ports to be displayed. **<portlist>** - Enter the list of ports to be displayed here.
cvid - (Optional) Specifies the rules for the specified CVIDs. **<vidlist>** - Enter the CVID value used here.

Restrictions

None.

Example

To display C-VLANs based on VLAN translation rules in the system:

```
DWS-3160-24PC:admin#show vlan_translation
Command: show vlan_translation

Port    CVID       SPVID      Action    Priority
-----   --------   --------   -------   ---------
1       2          3          Replace   -
1       3          2          Add       -

 Total Entries: 2

DWS-3160-24PC:admin#
```

Chapter 59 Quality of Service (QoS) Command List

config bandwidth_control [<portlist> | all] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit | <value 64-1024000>]}

show bandwidth_control {<portlist>}

config per_queue bandwidth_control {ports [<portlist> | all]} <cos_id_list 0-7> {{min_rate [no_limit | <value 64-1024000>]} max_rate [no_limit | <value 64-1024000>]}

show per_queue bandwidth_control {<portlist>}

config scheduling {ports [<portlist> | all]} <class_id 0-7> [strict | weight <value 1-127>]

config scheduling_mechanism {ports [<portlist> | all]} [strict | wrr]

show scheduling {<portlist>}

show scheduling_mechanism {<portlist>}

config 802.1p user_priority <priority 0-7> <class_id 0-7>

show 802.1p user_priority

config 802.1p default_priority [<portlist> | all] <priority 0-7>

show 802.1p default_priority {<portlist>}

enable hol_prevention

disable hol_prevention

show hol_prevention

config dscp trust [<portlist> | all] state [enable | disable]

show dscp trust {<portlist>}

config dscp map {[<portlist> | all]} [dscp_priority <dscp_list> to <priority 0-7> | dscp_dscp <dscp_list> to <dscp 0-63>]

show dscp map {<portlist>} [dscp_priority | dscp_dscp] {dscp <dscp_list>}

59-1 config bandwidth_control

Description

This command is used to configure the port bandwidth limit control.

Format

config bandwidth_control [<portlist> | all] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit | <value 64-1024000>]}

Parameters

<portlist> - Specifies a range of ports to be configured.
all – Specifies that all the ports will be used for this configuration.

rx_rate - (Optional) Specifies the limitation applied to receive data rate.
- **no_limit** - Indicates there is no limit on receiving bandwidth of the configured ports. The actual bandwidth will be an adjusted value based on the user specified bandwidth. The actual limit may be equal to the user specified limit, but will not exceed it. The actual limit recognized by the device, will be displayed when the command is executed.
- **<value 64-1024000>** - Enter the receiving data rate here. This value must be between 64 and 1024000 Kbits/sec.

tx_rate - (Optional) Specifies the limitation applied to transmit data rate.
- **no_limit** - Indicates there is no limit on port tx bandwidth. The actual bandwidth will be an adjusted value based on the user specified bandwidth. The actual limit may be equal to the user specified limit, but will not exceed it. The actual limit recognized by the device, will be displayed when the command is executed.

<value 64-1024000> - Enter the transmitting data rate here. This value must be between 64 and 1024000 Kbits/sec.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the port bandwidth:

```
DWS-3160-24PC:admin#config bandwidth_control 1-10 tx_rate 100
Command: config bandwidth_control 1-10 tx_rate 100

 Granularity: RX: 64, TX: 64. Actual Rate: TX: 64.

Success.

DWS-3160-24PC:admin#
```

59-2 show bandwidth_control

Description

This command is used to display the port bandwidth configurations. The bandwidth can also be assigned by the RADIUS server through the authentication process. If RADIUS server has assigned the bandwidth, then the RADIUS-assigned bandwidth will be the effective bandwidth. The authentication with the RADIUS sever can be per port or per user. For per-user authentication, there may be multiple bandwidth control values assigned when there are multiple users attached to this specific port. In this case, the largest assigned bandwidth value will be applied to the effective bandwidth for this specific port.

NOTE: Only devices that support MAC-based VLAN can provide per user authentication.

Format

show bandwidth_control {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be displayed.

If no parameter specified, system will display all ports bandwidth configurations.

Restrictions

None.

Example

To display port bandwidth control table:

```
DWS-3160-24PC:admin#show bandwidth_control 1-10
Command: show bandwidth_control 1-10

Bandwidth Control Table

Port   RX Rate       TX Rate       Effective RX       Effective TX
       (Kbit/sec)    (Kbit/sec)    (Kbit/sec)         (Kbit/sec)
-----  ----------    ----------    ----------------   ----------------
 1      No Limit     64            No Limit            64
 2      No Limit     64            No Limit            64
 3      No Limit     64            No Limit            64
 4      No Limit     64            No Limit            64
 5      No Limit     64            No Limit            64
 6      No Limit     64            No Limit            64
 7      No Limit     64            No Limit            64
 8      No Limit     64            No Limit            64
 9      No Limit     64            No Limit            64
 10     No Limit     64            No Limit            64

DWS-3160-24PC:admin#
```

59-3 config per_queue bandwidth_control

Description

This command is used to configure per port CoS bandwidth control.

Format

config per_queue bandwidth_control {ports [<portlist> | all]} <cos_id_list 0-7> {{min_rate [no_limit | <value 64-1024000>]} max_rate [no_limit | <value 64-1024000>]}

Parameters

ports - (Optional) Specifies a range of ports to be configured.
<portlist> - Enter the list of port used for this configuration here.
all - For set all ports in the system, you may use "all" parameter. If no parameter is specified, system will set all ports.

<cos_id_list 0-7> - Specifies a list of priority queues. The priority queue number is ranged from 0 to 7.

min_rate - (Optional) Specifies that one of the parameters below (no_limit or <value m-n) will be applied to the mini-rate at which the above specified class will be allowed to receive packets.
no_limit - Specifies that there will be no limit on the rate of packets received by the above specified class.
<value 64-1024000> - Specifies the packet limit, in Kbps, that the above ports will be allowed to receive. If the specified rate is not multiple of minimum granularity, the rate will be adjusted.

max_rate - (Optional) Specifies that one of the parameters below (no_limit or <value m-n >) will be applied to the maximum rate at which the above specified class will be allowed to transmit packets.
no_limit - Specifies that there will be no limit on the rate of packets received by the above specified class.
<value 64-1024000> - Specifies the packet limit, in Kbps, that the above ports will be allowed to receive. If the specified rate is not multiple of minimum granularity, the rate will be

adjusted.

Restrictions

Only Administrators can issue this command.

Example

To configure the ports 1-10 CoS bandwidth queue 1 min rate to 130 and max rate to 100000:

```
DWS-3160-24PC:admin#config per_queue bandwidth_control ports 1-10 1 min_rate
130 max_rate 1000
Command: config per_queue bandwidth_control ports 1-10 1 min_rate 130 max_rate
1000

 Granularity: TX: 64. Actual Rate: MIN: 128, MAX: 960.

Success.

DWS-3160-24PC:admin#
```

59-4 show per_queue bandwidth_control

Description

This command is used to display the per port CoS bandwidth control settings.

Format

show per_queue bandwidth_control {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be displayed.
If no parameter is specified, system will display all ports CoS bandwidth configurations.

Restrictions

None.

Example

Display per port CoS bandwidth control table:

```
DWS-3160-24PC:admin#show per_queue bandwidth_control 10
Command: show per_queue bandwidth_control 10

Queue Bandwidth Control Table On Port: 10

Queue     Min Rate(Kbit/sec)     Max Rate(Kbit/sec)
0         No Limit               No Limit
1         128                    960
2         No Limit               No Limit
3         No Limit               No Limit
4         No Limit               No Limit
5         No Limit               No Limit
6         No Limit               No Limit
7         No Limit               No Limit

DWS-3160-24PC:admin#
```

59-5 config scheduling

Description

This command is used to configure the traffic scheduling mechanism for each CoS queue.

Format

config scheduling {ports [<portlist> | all]} <class_id 0-7> [strict | weight <value 1-127>]

Parameters

ports - Specifies a range of ports to be configured.
<portlist> - Enter the list of port used for this configuration here.

<class_id 0-7> - This specifies the 8 hardware priority queues which the config scheduling command will apply to. The four hardware priority queues are identified by number from 0 to 7 with the 0 queue being the lowest priority.

strict - The queue will operate in strict mode.

weight - Specifies the weights for weighted round robin.
<value 1-127> - Enter the weights for weighted round robin value here. This value must be between 1 and 127.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the traffic scheduling CoS queue 1 to weight 25 on port 10:

```
DWS-3160-24PC:admin# config scheduling ports 10 1 weight 25
Command: config scheduling ports 10 1 weight 25

Success.

DWS-3160-24PC:admin#
```

59-6 config scheduling_mechanism

Description

This command is used to configure the traffic scheduling mechanism for each CoS queue.

Format

config scheduling_mechanism {ports [<portlist> | all]} [strict | wrr]

Parameters

ports - (Optional) Specifies a range of ports to be configured. **<portlist>** - Enter the list of port used for this configuration here. **all** - For set all ports in the system, you may use “all” parameter. If no parameter is specified, system will set all ports.
strict - All queues operate in strict mode.
wrr - Each queue operates based on its setting.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the traffic scheduling mechanism for each CoS queue:

```
DWS-3160-24PC:admin# config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DWS-3160-24PC:admin#
```

To configure the traffic scheduling mechanism for CoS queue on port 1:

```
DWS-3160-24PC:admin# config scheduling_mechanism ports 1 strict
Command: config scheduling_mechanism ports 1 strict

Success.

DWS-3160-24PC:admin#
```

59-7 show scheduling

Description

This command is used to display the current traffic scheduling parameters.

Format

show scheduling {<portlist>}

Parameters

<portlist> **-** (Optional) Specifies a range of ports to be displayed.
If no parameter specified, system will display all ports scheduling configurations.

Restrictions

None.

Example

To display the traffic scheduling parameters for each CoS queue on port 1(take eight hardware priority queues for example):

```
DWS-3160-24PC:admin#show scheduling 1
Command: show scheduling 1

QOS Output Scheduling On Port: 1
Class ID  Weight
--------  ------
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
Class-6   7
Class-7   8

DWS-3160-24PC:admin#
```

59-8 show scheduling_mechanism

Description

This command is used to display the traffic scheduling mechanism.

Format

show scheduling_mechanism {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be displayed.
If no parameter specified, system will display all ports scheduling mechanism configurations.

Restrictions

None.

Example

To display the scheduling mechanism for ports 1 to 5:

```
DWS-3160-24PC:admin#show scheduling_mechanism 1-5
Command: show scheduling_mechanism 1-5

Port    Mode
-----   ------
1       Strict
2       Strict
3       Strict
4       Strict
5       Strict

DWS-3160-24PC:admin#
```

59-9 config 802.1p user_priority

Description

This command is used to map the 802.1p user priority of an incoming packet to one of the eight hardware queues available on the Switch.

Format

config 802.1p user_priority <priority 0-7> <class_id 0-7>

Parameters

<priority 0-7> - The 802.1p user priority you want to associate with the <class_id> (the number of the hardware queue) with.

<class_id 0-7> - The number of the Switch’s hardware priority queue. The Switch has 8 hardware priority queues available. They are numbered between 0 (the lowest priority) and 7 (the highest priority).

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the 802.1p user priority:

```
DWS-3160-24PC:admin#config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DWS-3160-24PC:admin#
```

59-10 show 802.1p user_priority

Description

This command is used to display the 802.1p user priority for ports.

Format

show 802.1p user_priority

Parameters

None.

Restrictions

None.

Example

To display the 802.1p user priority:

```
DWS-3160-24PC:admin#show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic

Priority-0  ->  <Class-2>
Priority-1  ->  <Class-3>
Priority-2  ->  <Class-1>
Priority-3  ->  <Class-3>
Priority-4  ->  <Class-4>
Priority-5  ->  <Class-5>
Priority-6  ->  <Class-6>
Priority-7  ->  <Class-7>

DWS-3160-24PC:admin#
```

59-11 config 802.1p default_priority

Description

This command is used to configure the 802.1p default priority settings on the Switch. If an untagged packet is received by the Switch, the priority configured with this command will be written to the packet’s priority field.

Format

config 802.1p default_priority [<portlist> | all] <priority 0-7>

Parameters

<portlist> - This specifies a range of ports for which the default priority is to be configured. That is, a range of ports for which all untagged packets received will be assigned the priority specified below. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then highest Switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash.
all - Specifies that the command apply to all ports on the Switch.

<priority 0-7> - The priority value (0 to 7) assigned to untagged packets received by the Switch or a range of ports on the Switch.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the 802.1p default priority settings on the Switch:

```
DWS-3160-24PC:admin# config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DWS-3160-24PC:admin#
```

59-12 show 802.1p default_priority

Description

This command is used to display the current configured default priority settings on the Switch.

The default priority can also be assigned by the RADIUS server through the authentication process. The authentication with the RADIUS sever can be per port or port user. For per port authentication, the priority assigned by RADIUS server will be the effective port default priority. For per user authentication, the priority assigned by RADIUS will not be the effective port default priority whereas it will become the priority associated with MAC address.

NOTE: Only devices supporting MAC-based VLAN can provide per user authentication.

Format

show 802.1p default_priority {<portlist>}

Parameters

<portlist> - (Optional) Specified a range of ports to be displayed.

If no parameter is specified, all ports for 802.1p default priority will be displayed.

Restrictions

None.

Example

To display 802.1p default priority:

```
DWS-3160-24PC:admin#show 802.1p default_priority 1-10
Command: show 802.1p default_priority 1-10

Port       Priority     Effective Priority
----       -----------  ------------------
1          5            5
2          5            5
3          5            5
4          5            5
5          5            5
6          5            5
7          5            5
8          5            5
9          5            5
10         5            5

DWS-3160-24PC:admin#
```

59-13 enable hol_prevention

Description

This command is used to enable head-of-line (HOL) prevention on the Switch.

Format

enable hol_prevention

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable HOL prevention on the Switch:

```
DWS-3160-24PC:admin# enable hol_prevention
Command: enable hol_prevention

Success.

DWS-3160-24PC:admin#
```

59-14 disable hol_prevention

Description

This command is used to disable HOL prevention on the Switch.

Format

disable hol_prevention

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable HOL prevention on the Switch:

```
DWS-3160-24PC:admin# disable hol_prevention
Command: disable hol_prevention

Success.

DWS-3160-24PC:admin#
```

59-15 show hol_prevention

Description

This command is used to display the HOL prevention state on the Switch.

Format

show hol_prevention

Parameters

None.

Restrictions

None.

Example

To display HOL prevention state on the Switch.

```
DWS-3160-24PC:admin#show hol_prevention
Command: show hol_prevention

Device HOL Prevention State: Enabled


DWS-3160-24PC:admin#
```

59-16 config dscp trust

Description

This command is used to configure the state of DSCP trust per port. When DSCP is not trusted, 802.1p is trusted.

Format

config dscp trust [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter the list of port used for this configuration here.
all - Specifies that the command apply to all ports on the Switch.

state - Enable or disable to trust DSCP. By default, DSCP trust is disabled.
  enable - Specifies that the DSCP trust state will be enabled.
  disable - Specifies that the DSCP trust state will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable DSCP trust on ports 1-8.

```
DWS-3160-24PC:admin#config dscp trust 1-8 state enable
Command: config dscp trust 1-8 state enable

Success.

DWS-3160-24PC:admin#
```

59-17 show dscp trust

Description

This command is used to display the DSCP trust state for the specified port(s) on the Switch.

Format

show dscp trust {<portlist>}

Parameters

<portlist> - (Optional) A range of ports to display.

If not Specifies the port, all ports for DSCP trust status on the Switch will be displayed.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To display the DSCP trust status on ports 1-8:

```
DWS-3160-24PC:admin#show dscp trust 1-8
Command: show dscp trust 1-8

Port DSCP-Trust
---- ----------
1    Enabled
2    Enabled
3    Enabled
4    Enabled
5    Enabled
6    Enabled
7    Enabled
8    Enabled

DWS-3160-24PC:admin#
```

59-18 config dscp map

Description

This command is used to configure the mapping of DSCP priorities.

The mapping of DSCP to priority will be used to determine the priority of the packet (which will be then used to determine the scheduling queue) when the port is in DSCP trust state.

The mapping of DSCP to color will be used to determine the initial color of the packet when the policing function of the packet is color aware and the packet is DSCP-trusted.

The DSCP-to-DSCP mapping is used in the swap of DSCP of the packet when the packet is ingresses to the port. The remaining processing of the packet will base on the new DSCP. By default, the DSCP is mapped to the same DSCP.

These DSCP mapping will take effect at the same time when IP packet ingress from a DSCP-trusted port.

Format

config dscp map {[<portlist> | all]} [dscp_priority <dscp_list> to <priority 0-7> | dscp_dscp <dscp_list> to <dscp 0-63>]

Parameters

<portlist> - Enter the list of port used for this configuration here.
all - Specifies that all the ports will be included in this configuration.

dscp_priority - Specifies a list of DSCP value to be mapped to a specific priority.
<dscp_list> - Enter the DSCP priority list here.
to - Specifies that the above or following parameter will be mapped to the previously mentioned parameter.
<priority 0-7> - Specifies the result priority of mapping.

dscp_dscp - Specifies a list of DSCP value to be mapped to a specific DSCP.
<dscp_list> - Enter the DSCP to DSCP list here.
to - Specifies that the above or following parameter will be mapped to the previously mentioned parameter.
<dscp 0-63> - Specifies the result DSCP of mapping.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the mapping of the DSCP priority to priority 1:

```
DWS-3160-24PC:admin#config dscp map 1-8 dscp_priority 1 to 1
Command: config dscp map 1-8 dscp_priority 1 to 1

Success.

DWS-3160-24PC:admin#
```

To configure the global mapping of the DSCP priority to priority 1:

```
DWS-3160-24PC:admin#config dscp map dscp_priority 1 to 1
Command: config dscp map dscp_priority 1 to 1

Success.

DWS-3160-24PC:admin#
```

59-19 show dscp map

Description

This command is used to display the DSCP trusted port list and mapped color priority.

Format

show dscp map {<portlist>} [dscp_priority | dscp_dscp] {dscp <dscp_list>}

Parameters

<portlist> - (Optional) A range of ports to display. If no parameter is specified, all ports' dscp mapping will be displayed.

dscp_priotity - Specifies a list of DSCP value to be mapped to a specific priority.
dscp_dscp - Specifies a list of DSCP value to be mapped to a specific DSCP.

dscp - (Optional) This specifies DSCP value that will be mapped.
<dscp_list> - Enter the DSCP list here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To display DSCP map configuration on port 1.

```
DWS-3160-24PC:admin#show dscp map 1 dscp_dscp
Command: show dscp map 1 dscp_dscp

DSCP to DSCP Mapping:
--------------------------------------------------------------
Port 1     |   0    1    2    3    4    5    6    7    8    9
-----------+--------------------------------------------------
         0 |   0    1    2    3    4    5    6    7    8    9
         1 |  10   11   12   13   14   15   16   17   18   19
         2 |  20   21   22   23   24   25   26   27   28   29
         3 |  30   31   32   33   34   35   36   37   38   39
         4 |  40   41   42   43   44   45   46   47   48   49
         5 |  50   51   52   53   54   55   56   57   58   59
         6 |  60   61   62   63
--------------------------------------------------------------


DWS-3160-24PC:admin#
```

Chapter 60 Remote Switched Port Analyzer (RSPAN) Command List

enable rspan
disable rspan
create rspan vlan [vlan_name <vlan_name> | vlan_id <value 1-4094>]
delete rspan vlan [vlan_name <vlan_name> | vlan_id <value 1-4094>]
config rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>] [redirect [add | delete] ports <portlist> | source {[add | delete] ports <portlist> [rx | tx | both]}]
show rspan {[vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]}

60-1 enable rspan

Description

This command is used to enable the RSPAN function. The purpose of the RSPAN function is to mirror packets to a remote Switch.

A packet travels from the Switch where the monitored packet is received, passing through the intermediate Switch, and then to the Switch where the sniffer is attached. The first Switch is also named the source Switch.

To make the RSPAN function work, the RSPAN VLAN source setting must be configured on the source Switch. For the intermediate and the last Switch, the RSPAN VLAN redirect setting must be configured.

NOTE: RSPAN VLAN mirroring will only work when RSPAN is enabled (when one RSPAN VLAN has been configured with a source port).

The RSPAN redirect function will work when RSPAN is enabled and at least one RSPAN VLAN has been configured with redirect ports.

Format

enable rspan

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the RSPAN function:

```
DWS-3160-24PC:admin# enable rspan
Command: enable rspan

Success.

DWS-3160-24PC:admin#
```

60-2 disable rspan

Description

This command is used to disable the RSPAN function.

Format

disable rspan

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the RSPAN function:

```
DWS-3160-24PC:admin# disable rspan
Command: disable rspan

Success.

DWS-3160-24PC:admin#
```

60-3 create rspan vlan

Description

This command is used to create an RSPAN VLAN. Up to 16 RSPAN VLANs can be created.

Format

create rspan vlan [vlan_name <vlan_name> | vlan_id <value 1-4094>]

Parameters

vlan_name - Create the RSPAN VLAN by VLAN name.
  <vlan_name> - Enter the VLAN name here.

vlan_id - Create the RSPAN VLAN by VLAN ID.
  <value 1-4094> - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create an RSPAN VLAN entry by VLAN name “v2”:

```
DWS-3160-24PC:admin# create rspan vlan vlan_name v2
Command: create rspan vlan vlan_name v2

Success.

DWS-3160-24PC:admin#
```

To create an RSPAN VLAN entry by VLAN ID “3”:

```
DWS-3160-24PC:admin# create rspan vlan vlan_id 3
Command: create rspan vlan vlan_id 3

Success.

DWS-3160-24PC:admin#
```

60-4 delete rspan vlan

Description

This command is used to delete an RSPAN VLAN.

Format

delete rspan vlan [vlan_name <vlan_name> | vlan_id <value 1-4094>]

Parameters

vlan_name - Delete RSPAN VLAN by VLAN name.
  <vlan_name> - Enter the VLAN name here.

vlan_id - Delete RSPAN VLAN by VLAN ID.
  <value 1-4094> - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an RSPAN VLAN entry by VLAN name “v2”:

```
DWS-3160-24PC:admin# delete rspan vlan vlan_name v2
Command: delete rspan vlan vlan_name v2

Success.

DWS-3160-24PC:admin#
```

To delete an RSPAN VLAN entry by VLAN ID “3”:

```
DWS-3160-24PC:admin# delete rspan vlan vlan_id 3
Command: delete rspan vlan vlan_id 3

Success.

DWS-3160-24PC:admin#
```

60-5 config rspan vlan

Description

This command is used to configure the source setting for the RSPAN VLAN on the source Switch or configures the redirect port on the intermediate Switch and destination Switch.

Format

config rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>] [redirect [add | delete] ports <portlist> | source {[add | delete] ports <portlist> [rx | tx | both]}]

Parameters

vlan - Specifies the RSPAN VLAN used for this configuration.

vlan_name - Specifies the RSPAN VLAN by VLAN name.
<vlan_name> - Enter the VLAN name here.

vlan_id - Specifies the RSPAN VLAN by VLAN ID.
<value 1-4094> - Enter the VLAN ID here. This value must be between 1 and 4094.

redirect - Specifies output portlist for the RSPAN VLAN packets. If the redirect port is a Link Aggregation port, there will perform the Link Aggregation behavior for RSPAN packets.
add - Specifies to add output ports for the RSPAN VLAN packets.
delete - Specifies to delete output ports for the RSPAN VLAN packets.

ports - Specifies the output ports for the RSPAN VLAN packets.
<portlist> - Enter the list of ports that will be used for this configuration here.

source - If the ports are not specified by this command, the source of RSPAN will come from the source specified by the mirror command or the flow-based source specified by an ACL. If no parameter is specified for source, it deletes the configured source parameters.

add - (Optional) Add source ports.
delete - (Optional) Delete source ports.

ports - (Optional) Specifies source portlist to add to or delete from the RSPAN source
<portlist> - Enter the list of ports that will be used for this configuration here.

rx - (Optional) Only monitor ingress packets.
tx - (Optional) Only monitor egress packets.
both - (Optional) Monitor both ingress and egress packets.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure an RSPAN source entry without source target port:

```
DWS-3160-24PC:admin#config rspan vlan vlan_name v2 source add ports 2-5 rx
Command: config rspan vlan vlan_name v2 source add ports 2-5 rx

Success.

DWS-3160-24PC:admin#
```

To configure an RSPAN source entry for per flow RSPAN, without any source ports:

```
DWS-3160-24PC:admin#config rspan vlan vlan_id 2 source
Command: config rspan vlan vlan_id 2 source

Success.

DWS-3160-24PC:admin#
```

To add redirect ports for special RSPAN VLAN on intermediate or destination Switch:

```
DWS-3160-24PC:admin#config rspan vlan vlan_name v2 redirect add ports 18-19
Command: config rspan vlan vlan_name v2 redirect add ports 18-19

Success.

DWS-3160-24PC:admin#config rspan vlan vlan_id 2 redirect add ports 18-19
Command: config rspan vlan vlan_id 2 redirect add ports 18-19

Success.

DWS-3160-24PC:admin#
```

60-6 show rspan

Description

This command is used to display the RSPAN configuration.

Format

show rspan {[vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]}

Parameters

vlan_name - (Optional) Specifies the RSPAN VLAN by VLAN name

<vlan_name> - Enter the VLAN name here.

vlan_id - (Optional) Specifies the RSPAN VLAN by VLAN ID.

<value 1-4094> - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

None.

Example

To display the RSPAN settings:

```
DWS-3160-24PC:admin#show rspan
Command: show rspan

RSPAN   : Enabled

RSPAN VLAN ID  : 2
--------------------
  Source Port
      RX           : 2-5
      TX           :
  Redirect Port    : 18-19

RSPAN VLAN ID  : 3
--------------------

Total RSPAN VLAN :2

DWS-3160-24PC:admin#
```

Chapter 61 Safeguard Engine Command List

config safeguard_engine {state [enable | disable]| utilization {rising <20-100> | falling <20-100>} | trap_log [enable | disable] | mode [strict | fuzzy]}

show safeguard_engine

61-1 config safeguard_engine

Description

This command is used to configure the CPU protection control for the system.

Format

config safeguard_engine {state [enable | disable]| utilization {rising <20-100> | falling <20-100>} | trap_log [enable | disable] | mode [strict | fuzzy]}

Parameters

state - (Optional) Specifies to configure CPU protection state to enable or disable.
enable - Specifies that CPU protection will be enabled.
disable - Specifies that CPU protection will be enabled.

utilization - (Optional) Specifies to configure the CPU protection threshold.
rising - Config utilization rising threshold , the range is between 20%-100% , if the CPU utilization is over the rising threshold, the Switch enters exhausted mode.
<20-100> - Enter the utilization rising value here. This value must be between 20 and 100.
falling - Config utilization falling threshold , the range is between 20%-100% , if the CPU utilization is lower than the falling threshold, the Switch enters normal mode.
<20-100> - Enter the utilization falling value here. This value must be between 20 and 100.

trap_log - (Optional) Configure the state of CPU protection related trap/log mechanism to enable or disable. If set to enable, trap and log will be active while cpu protection current mode changed. If set to disable, current mode change will not trigger trap and log events.
enable - Specifies that the CPU protection trap or log mechanism will be enabled.
disable - Specifies that the CPU protection trap or log mechanism will be disabled.

mode - (Optional) determine the controlling method of broadcast traffic. Here are two modes (strict and fuzzy).
strict - In strict, the Switch will stop receiving all 'ARP not to me' packets (the protocol address of target in ARP packet is the Switch itself). That means no matter what reasons cause the high CPU utilization (may not caused by ARP storm), the Switch reluctantly processes any 'ARP not to me' packets in exhausted mode.
fuzzy - In fuzzy mode, the Switch will adjust the bandwidth dynamically depend on some reasonable algorithm.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure CPU protection:

```
DWS-3160-24PC:admin# config safeguard_engine state enable utilization rising 50
falling 30 trap_log enable
Command: config safeguard_engine state enable utilization rising 50 falling 30
trap_log enable

Success.

DWS-3160-24PC:admin#
```

61-2 show safeguard_engine

Description

This command is used to display safeguard engine information.

Format

show safeguard_engine

Parameters

None.

Restrictions

None.

Example

To display safeguard_engine information:

```
DWS-3160-24PC:admin#show safeguard_engine
Command: show safeguard_engine

Safeguard Engine State          :  Enabled
Safeguard Engine Current Status :  Normal Mode
=======================================================
CPU Utilization Information:
Rising Threshold  :  50%
Falling Threshold :  30%
Trap/Log State    :  Enabled
Mode              :  Fuzzy

DWS-3160-24PC:admin#
```

NOTE: The Safeguard Engine has two status modes called exhausted mode and normal mode.

Chapter 62 Secure Shell (SSH) Command List

config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5| SHA1 | RSA | DSA] [enable | disable]
show ssh algorithm
config ssh authmode [password | publickey | hostbased] [enable | disable]
show ssh authmode
config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> [<ipaddr> | <ipv6addr>]] | password | publickey]
show ssh user authmode
config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}
enable ssh
disable ssh
show ssh server

62-1 config ssh algorithm

Description

This command is used to configure the SSH service algorithm.

Format

config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5| SHA1 | RSA | DSA] [enable | disable]

Parameters

3DES - The "3DES" cipher is three-key triple-DES (encrypt-decrypt-encrypt), where the first 8 bytes of the key are used for the first encryption, the next 8 bytes for the decryption, and the following 8 bytes for the final encryption.
AES (128,192,256) - Advanced Encryption Standard.
arcfour - RC4 (also known as ARC4 or ARCFOUR meaning Alleged RC4) is the most widely-used software stream cipher.
blowfish - Blowfish is a keyed, symmetric block cipher.

cast128 - CAST-128 is a 12- or 16-round feistel network with a 64-bit block size and a key size of between 40 to 128 bits.
twofish (128,192,256) - Twofish has a 128-bit block size, a key size ranging from 128 to 256 bits.
MD5 - Message-Digest Algorithm 5.
SHA1 - Secure Hash Algorithm.
RSA - RSA encryption algorithm is a non-symmetric encryption algorithm.
DSS - Digital Signature Standard.

enable - Enabled the algorithm.
disable - Disables the algorithm.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable SSH server public key algorithm:

```
DWS-3160-24PC:admin#config ssh algorithm DSA enable
Command: config ssh algorithm DSA enable

Success.

DWS-3160-24PC:admin#
```

62-2 show ssh algorithm

Description

This command is used to display the SSH service algorithm.

Format

show ssh algorithm

Parameters

None.

Restrictions

None.

Example

To display server algorithm:

```
DWS-3160-24PC:admin#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
--------------------------
3DES       : Enabled
AES128     : Enabled
AES192     : Enabled
AES256     : Enabled
Arcfour    : Enabled
Blowfish   : Enabled
Cast128    : Enabled
Twofish128 : Enabled
Twofish192 : Enabled
Twofish256 : Enabled

Data Integrity Algorithm
--------------------------
MD5        : Enabled
SHA1       : Enabled

Public Key Algorithm
--------------------------
RSA        : Enabled
DSA        : Enabled

DWS-3160-24PC:admin#
```

62-3 config ssh authmode

Description

This command is used to configure the user authentication method for SSH.

Format

config ssh authmode [password | publickey | hostbased] [enable | disable]

Parameters

password - Specifies user authentication method. **publickey** - Specifies user authentication method. **hostbased** - Specifies user authentication method.
enable - Enable user authentication method. **disable** - Disable user authentication method.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure user authentication method:

```
DWS-3160-24PC:admin# config ssh authmode publickey enable
Command: config ssh authmode publickey enable

Success.

DWS-3160-24PC:admin#
```

62-4 show ssh authmode

Description

This command is used to display the user authentication method.

Format

show ssh authmode

Parameters

None.

Restrictions

None.

Example

To display user authentication method:

```
DWS-3160-24PC:admin#show ssh authmode
Command: show ssh authmode

The SSH Authentication Method:
Password    : Enabled
Public Key  : Enabled
Host-based  : Enabled

DWS-3160-24PC:admin#
```

62-5 config ssh user

Description

This command is used to configure user information for SSH.

Format

config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> [<ipaddr> | <ipv6addr>]] | password | publickey]

Parameters

user - Specifies the user name.
  <username 15> - Enter the user name used here. This name can be up to 15 characters long.

hostbased - Specifies user authentication method.
  hostname - Specifies host domain name.
    <domain_name 32> - Enter the domain name here. This name can be up to 32 characters long.
  hostname_IP - Specifies host domain name and IP address.
    <domain_name 32> - Specifies host name if configuring Host-based method.

<ipaddr> - Specifies host IP address if configuring Host-based method.
<ipv6addr> - Specifies host IPv6 address if configuring Host-based method.

password - Specifies user authentication method.

publickey - Specifies user authentication method.

Restrictions

Only Administrators can issue this command.

Example

To update the user, called ‘superuser’, authentication method:

```
DWS-3160-24PC:admin#config ssh user superuser authmode publickey
Command: config ssh user superuser authmode publickey

Success.

DWS-3160-24PC:admin#
```

62-6 show ssh user

Description

This command is used to display the SSH user information.

Format

show ssh user authmode

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display user information about SSH configuration:

```
DWS-3160-24PC:admin#show ssh user authmode
Command: show ssh user authmode

Current Accounts:
User Name       Authentication Host Name                          Host IP
--------------- ---------      -------------------------------- ---------------
admin           Password
oper            Host-based     localhost                        10.90.90.200
power           Host-based     localhost
superuser       Public Key
user            Password

Total Entries : 5

DWS-3160-24PC:admin#
```

62-7 config ssh server

Description

This command is used to configure the SSH server general information.

Format

config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}

Parameters

maxsession - (Optional) Specifies SSH server maximum session at the same time, maximum 8 sessions.
<int 1-8> - Enter the maximum session value here. This value must be between 1 and 8.

contimeout - (Optional) Specifies SSH server connection time-out, in the unit of second.
<sec 120-600> - Enter the connection time-out value here. This value must be between 120 and 600 seconds.

authfail - (Optional) Specifies user maximum fail attempts.
<int 2-20> - Enter the user maximum fail attempts value here. This value must be between 2 and 20.

rekey - (Optional) Specifies time to re-generate session key. There are 10 minutes, 30 minutes, 60 minutes and never for the selection, which means do NOT re- generate session key
10min - Specifies that the re-generate session key time will be 10 minutes.
30min - Specifies that the re-generate session key time will be 30 minutes.
60min - Specifies that the re-generate session key time will be 60 minutes.
never - Specifies that the re-generate session key time will be set to never.

port - (Optional) Specifies the TCP port used to communication between SSH client and server. The default value is 22.
<tcp_port_number 1-65535> - Enter the TCP port number here. This value must be between 1 and 65535.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure SSH server maximum session number is 3:

```
DWS-3160-24PC:admin# config ssh server maxsession 3
Command: config ssh server maxsession 3

Success.

DWS-3160-24PC:admin#
```

62-8 enable ssh

Description

This command is used to enable SSH server services. When enabling SSH, TELNET will be disabled.

Format

enable ssh

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the SSH server:

```
DWS-3160-24PC:admin# enable ssh
Command: enable ssh

Success.

DWS-3160-24PC:admin#
```

62-9 disable ssh

Description

This command is used to disable SSH server services.

Format

disable ssh

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the SSH server services:

```
DWS-3160-24PC:admin# disable ssh
Command: disable ssh

Success.

DWS-3160-24PC:admin#
```

62-10 show ssh server

Description

This command is used to display the SSH server general information.

Format

show ssh server

Parameters

None.

Restrictions

None.

Example

To display SSH server:

```
DWS-3160-24PC:admin#show ssh server
Command: show ssh server

The SSH Server Configuration
Maximum Session              : 3
Connection Timeout           : 120
Authentication Fail Attempts : 2
Rekey Timeout                : Never
TCP Port Number              : 22

DWS-3160-24PC:admin#
```

Chapter 63 Secure Sockets Layer (SSL) Command List

download ssl certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>
enable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
disable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
show ssl {certificate}
show ssl cachetimeout
config ssl cachetimeout <value 60-86400>

63-1 download ssl certificate

Description

This command is used to download the certificate to the device according to the certificate level. The user can download the specified certificate to the device which must, according to desired key exchange algorithm. For RSA key exchange, the user must download RSA type certificate and for DHS_DSS is using the DSA certificate for key exchange.

Format

download ssl certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>

Parameters

<ipaddr> - Enter the TFTP server IP address used for this configuration here.
certfilename - Specifies the desired certificate file name. **<path_filename 64>** - Certificate file path respect to TFTP server root path, and input characters max to 64 octets.
keyfilename - Specifies the private key file name which accompany with the certificate. **<path_filename 64>** - Private key file path respect to TFTP server root path, and input characters max to 64 octets.

Restrictions

Only Administrators can issue this command.

Example

To download a certificate from the TFTP server:

```
DWS-3160-24PC:admin# download ssl certificate 10.55.47.1 certfilename cert.der
keyfilename pkey.der
Command: download ssl certificate 10.55.47.1 certfilename cert.der keyfilename
pkey.der

Success.

DWS-3160-24PC:admin#
```

63-2 enable ssl

Description

This command is used to configure the SSL status and it’s ciphersuites. This will enable the SSL feature that include SSLv3 and TLSv1. For each cipher suites, user must specify it by using this command. The Web User Interface will be disabled when SSL is enabled.

Format

enable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}

Parameters

ciphersuite - (Optional) Specifies the cipher suite combination used for this configuration.

- **RSA_with_RC4_128_MD5** - Indicate RSA key exchange with RC4 128 bits encryption and MD5 hash.
- **RSA_with_3DES_EDE_CBC_SHA** - Indicate RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **DHE_DSS_with_3DES_EDE_CBC_SHA** - Indicate DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **RSA_EXPORT_with_RC4_40_MD5** - Indicate RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.

Restrictions

Only Administrators can issue this command.

Example

To enable the SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DWS-3160-24PC:admin# enable ssl ciphersuite RSA_with_RC4_128_MD5
Command: enable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DWS-3160-24PC:admin#
```

To enable SSL:

```
DWS-3160-24PC:admin#enable ssl
Command: enable ssl

Note: Web will be disabled if SSL is enabled.
Success.

DWS-3160-24PC:admin#
```

63-3 disable ssl

Description

This command is used to configure SSL feature and supported cipher suites. This will disable the SSL feature and for each cipher suites status the user must specify it by using this command.

Format

disable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}

Parameters

ciphersuite - (Optional) Specifies the cipher suite combination used for this configuration.

- **RSA_with_RC4_128_MD5** - Indicate RSA key exchange with RC4 128 bits encryption and MD5 hash.
- **RSA_with_3DES_EDE_CBC_SHA** - Indicate RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **DHE_DSS_with_3DES_EDE_CBC_SHA** - Indicate DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **RSA_EXPORT_with_RC4_40_MD5** - Indicate RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.

Restrictions

Only Administrators can issue this command.

Example

To disable SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DWS-3160-24PC:admin# disable ssl ciphersuite RSA_with_RC4_128_MD5
Command: disable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DWS-3160-24PC:admin#
```

To disable SSL:

```
DWS-3160-24PC:admin# disable ssl
Command: disable ssl

Success.

DWS-3160-24PC:admin#
```

63-4 show ssl

Description

This command is used to display the certificate status. User must download specified certificate type according to desired key exchange algorithm. The options may be no certificate, RSA type or DSA type certificate

Format

show ssl {certificate}

Parameters

certificate – (Optional) Specifies that the SSL certificate will be displayed.

Restrictions

None.

Example

To display SSL:

```
DWS-3160-24PC:admin#show ssl
Command: show ssl

 SSL Status                                     Enabled

 RSA_WITH_RC4_128_MD5                           Enabled
 RSA_WITH_3DES_EDE_CBC_SHA                      Enabled
 DHE_DSS_WITH_3DES_EDE_CBC_SHA                  Enabled
 RSA_EXPORT_WITH_RC4_40_MD5                     Enabled

DWS-3160-24PC:admin#
```

To display certificate:

```
DWS-3160-24PC:admin#show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DWS-3160-24PC:admin#
```

63-5 show ssl cachetimeout

Description

This command is used to display the cached timeout value which is designed for the ‘dlktimer’ library to remove the session ID after expiration. In order to support the ‘resume session’ feature, the SSL library keeps the session ID in web server, and invokes the ‘dlktimer’ library to remove this session ID by caching a timeout value.

Format

show ssl cachetimeout

Parameters

None.

Restrictions

None.

Example

To display SSL cache timeout:

```
DWS-3160-24PC:admin#show ssl cachetimeout
Command: show ssl cachetimeout

 Cache timeout is 600 second(s)

DWS-3160-24PC:admin#
```

63-6 config ssl cachetimeout

Description

This command is used to configure the cached timeout value which is designed for the ‘dlktimer’ library to remove the session ID after expiration. In order to support the ‘resume session’ feature, the SSL library keeps the session ID in web server, and invokes the ‘dlktimer’ library to remove this session ID by caching a timeout value.

Format

config ssl cachetimeout <value 60-86400>

Parameters

timeout - Specifies the SSL cache timeout value attributes.

<value 60-86400> - Enter the timeout value here. This value must be between 60 and 86400 seconds. The default value is 600 seconds.

Restrictions

Only Administrators can issue this command.

Example

To configure the SSL cache timeout value to 60:

```
DWS-3160-24PC:admin# config ssl cachetimeout 60
Commands: config ssl cachetimeout 60

Success.

DWS-3160-24PC:admin#
```

Chapter 64 sFlow Command List

create sflow flow_sampler ports [<portlist> | all] analyzer_server_id <value 1-4> {rate <value 0-65535> | maxheadersize <value 18-256>}

config sflow flow_sampler ports [<portlist> | all] {rate <value 0-65535> | maxheadersize <value 18-256>}

delete sflow flow_sampler ports [<portlist> | all]

create sflow counter_poller ports [<portlist> | all] analyzer_server_id <value 1-4> {interval [disable | <sec 20-120>]}

config sflow counter_poller ports [<portlist> | all] interval [disable | <sec 20-120>]

delete sflow counter_poller ports [<portlist> | all]

create sflow analyzer_server <value 1-4> owner <name 16> {timeout [<sec 1-2000000> | infinite] | collectoraddress <ipaddr> | collectorport <udp_port_number 1-65535> | maxdatagramsize <value 300-1400>}

config sflow analyzer_server <value 1-4> {timeout [<sec 1-2000000> | infinite] | collectoraddress <ipaddr> | collectorport <udp_port_number 1-65535> | maxdatagramsize <value 300-1400>}

delete sflow analyzer_server <value 1-4>

enable sflow

disable sflow

show sflow

show sflow flow_sampler

show sflow counter_poller

show sflow analyzer_server

64-1 create sflow flow_sampler

Description

This command is used to create the sFlow flow sampler. By configuring the sampling function for a port, a sample packet received by this port will be encapsulated and forwarded to analyzer server at the specified interval.

Format

create sflow flow_sampler ports [<portlist> | all] analyzer_server_id <value 1-4> {rate <value 0-65535> | maxheadersize <value 18-256>}

Parameters

ports - Specifies the list of ports to be configured.
<portlist> - Enter the list of ports that will be used for this configuration here.
all - Specifies all ports on the Switch.

analyzer_server_id - Specifies the ID of a server analyzer where the packet will be forwarded.
<value 1-4> - Enter the analyzer server ID here. This value must be between 1 and 4.

rate - (Optional) The sampling rate for packet Rx sampling. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0.
<value 0-65535> - Enter the sampling rate value here. This value must be between 0 and 65535.

maxheadersize - (Optional) The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. If not specified, the default value is 128.
<value 18-256> - Enter the maximum header size here. This value must be between 18 and 256.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create an sFlow flow sampler:

```
DWS-3160-24PC:admin# create sflow flow_sampler ports 1 analyzer_server_id 1
rate 1 maxheadersize 18
Command: create sflow flow_sampler ports 1 analyzer_server_id 1 rate 1
maxheadersize 18

Success.

DWS-3160-24PC:admin#
```

64-2 config sflow flow_sampler

Description

This command is used to configure the sFlow flow sampler parameters. In order to change the analyzer server ID, the user needs to delete the flow sampler first and then create a new one.

Format

config sflow flow_sampler ports [<portlist> | all] {rate <value 0-65535> | maxheadersize <value 18-256>}

Parameters

ports - Specifies the list of ports to be configured.
<portlist> - Enter the list of ports that will be used for this configuration here.
all - Specifies all ports on the Switch.

rate - (Optional) The sampling rate for packet Rx sampling. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0.
<value 0-65535> - Enter the sampling rate value here. This value must be between 0 and 65535.

maxheadersize - (Optional) The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. If not specified, the default value is 128.
<value 18-256> - Enter the maximum header size value here. This value must be between 18 and 256.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the sFlow sampler the rate of port 1 to be 0:

```
DWS-3160-24PC:admin#config sflow flow_sampler ports 1 rate 0 maxheadersize 18
Command: config sflow flow_sampler ports 1 rate 0 maxheadersize 18

Success.

DWS-3160-24PC:admin#
```

64-3 delete sflow flow_sampler

Description

This command is used to delete the sFlow flow sampler.

Format

delete sflow flow_sampler ports [<portlist> | all]

Parameters

ports - Specifies the list of ports to be configured.
<portlist> - Enter the list of ports that will be used for this configuration here.
all - Specifies all ports on the Switch.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the sFlow sampler port 1:

```
DWS-3160-24PC:admin# delete sflow flow_sampler ports 1
Command: delete sflow flow_sampler ports 1

Success.

DWS-3160-24PC:admin#
```

64-4 create sflow counter_poller

Description

This command is used to create the sFlow counter poller. The poller function instructs the Switch to forward statistics counter information with respect to a port.

Format

create sflow counter_poller ports [<portlist> | all] analyzer_server_id <value 1-4> {interval [disable | <sec 20-120>]}

Parameters

ports - Specifies the list of ports to be configured.

<portlist> - Enter the list of ports that will be used for this configuration here.

all - Specifies all ports on the Switch.

analyzer_server_id - The ID of a analyzer server.

<value 1-4> - Enter the analyzer server IS here. This value must be between 1 and 4.

interval - (Optional) The maximum number of seconds between successive statistics counters information.

disable - This new sFlow counter will not export counter until the interval to be set a appropriate value. If interval is not specified, its default value is disabled.

<sec 20-120> - Enter the maximum number of seconds between successive statistics counters information here. This value must be between 20 and 120 seconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create an sFlow counter poller, which sample port 1 to analyzer server 1:

```
DWS-3160-24PC:admin# create sflow counter_poller ports 1 analyzer_server_id 1
Command: create sflow counter_poller ports 1 analyzer_server_id 1

Success.

DWS-3160-24PC:admin#
```

64-5 config sflow counter_poller

Description

This command is used to configure the sFlow counter poller parameters. If the user wants the change the analyzer server ID, the counter poller must be removed first and then create a new one.

Format

config sflow counter_poller ports [<portlist> | all] interval [disable | <sec 20-120>]

Parameters

ports - Specifies the list of ports to be configured.

<portlist> - Enter the list of ports that will be used for this configuration here.

all - Specifies all ports on the Switch.

interval - The maximum number of seconds between successive samples of the counters.

disable - Stop exporting counter.

<sec 20-120> - Enter the maximum number of seconds between successive samples of the counters here. This value must be between 20 and 120.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the interval of sFlow counter poller port 1 to be 0:

```
DWS-3160-24PC:admin# config sflow counter_poller ports 1 interval disable
Command: config sflow counter_poller ports 1 interval disable

Success.

DWS-3160-24PC:admin#
```

64-6 delete sflow counter_poller

Description

This command is used to delete an sFlow counter poller from a specified port.

Format

delete sflow counter_poller ports [<portlist> | all]

Parameters

ports - Specifies the list of ports to delete the counter poller.
<portlist> - Enter the list of ports that will be used for this configuration here.
all - Specifies all ports on the Switch.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete sFlow counter poller on port 1:

```
DWS-3160-24PC:admin# delete sflow counter_poller ports 1
Command: delete sflow counter_poller ports 1

Success.

DWS-3160-24PC:admin#
```

64-7 create sflow analyzer_server

Description

This command is used to create the analyzer server. The user can specify more than one analyzer server with the same IP address but with different UDP port numbers. You can have up to four unique combinations of IP addresses and UDP port numbers.

Format

create sflow analyzer_server <value 1-4> owner <name 16> {timeout [<sec 1-2000000> | infinite] | collectoraddress <ipaddr> | collectorport <udp_port_number 1-65535> | maxdatagramsize <value 300-1400>}

Parameters

analyzer_server - The ID of analyzer server.
<value 1-4> - Enter the analyzer server ID here.

owner - The entity making use of this sFlow analyzer_server. When owner is set or modified, the timeout value will become 400 automatically.
<name 16> - Enter the owner name here. This name can be up to 16 characters long.

timeout - (Optional) The seconds to wait before the server is timed out. When the analyzer server times out, all of the flow samplers and counter pollers associated with this analyzer server will be deleted. The default value is 400 seconds.
<sec 1-2000000> - Enter the time-out value here. This value must be between 1 and 2000000 seconds.
infinite - Indicates the analyzer server never timeout.

collectoraddress - (Optional) The IP or IPv6 address of the analyzer server. If this is set to 0 or not specified, the IP address is 0 and the entry is not active.
<ipaddr> - Enter the IP address used for the configuration here.

collectorport - (Optional) The destination UDP port for sending the sFlow datagram. If not specified, the default value is 6364. The specified UDP port number can NOT conflict with other applications.
<udp_port_number 1-65535> - Enter the destination UDP port number here. This value must be between 1 and 65535.

maxdatagramsize - (Optional) The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400 bytes.
<value 300-1400> - Enter the maximum datagram size here. This value must be between 300 and 1400.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create the analyzer server:

```
DWS-3160-24PC:admin# create sflow analyzer_server 2 owner monitor timeout
infinite collectoraddress 10.0.0.1 collectorport 65524 maxdatagramsize 300
Command: create sflow analyzer_server 2 owner monitor timeout infinite
collectoraddress 10.0.0.1 collectorport 65524 maxdatagramsize 300


Success.


DWS-3160-24PC:admin#
```

64-8 config sflow analyzer_server

Description

This command is used to configure the receiver information. The user can specify more than one collector with the same IP address if the UDP port numbers are unique.

Format

config sflow analyzer_server <value 1-4> {timeout [<sec 1-2000000> | infinite] | collectoraddress <ipaddr> | collectorport <udp_port_number 1-65535> | maxdatagramsize <value 300-1400>}

Parameters

analyzer_server - The ID of analyzer server.
<value 1-4> - Enter the analyzer server ID here. This value must be between 1 and 4.

timeout - (Optional) The time (in seconds) remaining before the sample is released and stops sampling. When the analyzer_server times out, all of the flow_samplers and counter pollers associated with this analyzer_server will be deleted.
<sec 1-2000000> - Enter the time-out value here. This value must be between 1 and 2000000 seconds.
infinity - Indicates the analyzer server never timeout

collectoraddress - (Optional) The IP address of the server. If not specified or set a 0 address, sFlow packets will not be sent to this server.
<ipaddr> - Enter the IP address used for the configuration here.

collectorport - (Optional) The destination UDP port for sending the sFlow datagram. If not specified, the default value is 6364
<udp_port_number 1-65535> - Enter the destination port number here. This value must be between 1 and 65535.

maxdatagramsize - (Optional) The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400 bytes.
<value 300-1400> - Enter the maximum datagram size here. This value must be between 300 and 1400.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the host 10.90.90.90 to be the sFlow analyzer server with the ID 1:

```
DWS-3160-24PC:admin# config sflow analyzer_server 1 collectoraddress
10.90.90.90
Command: config sflow analyzer_server 1 collectoraddress 10.90.90.90

Success.

DWS-3160-24PC:admin#
```

64-9 delete sflow_analyzer_server

Description

This command is used to delete a specified analyzer server.

Format

delete sflow analyzer_server <value 1-4>

Parameters

analyzer_server - The ID of analyzer server that to be deleted.
<value 1-4> - Enter the analyzer server ID value here. This value must be between 1 and 4.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an analyzer server:

```
DWS-3160-24PC:admin# delete sflow analyzer_server 1
Command: delete sflow analyzer_server 1

Success.

DWS-3160-24PC:admin#
```

64-10 enable sflow

Description

This command is used to enable the sFlow function on the Switch.

Format

enable sflow

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable sFlow globally:

```
DWS-3160-24PC:admin# enable sflow
Command: enable sflow

Success.

DWS-3160-24PC:admin#
```

64-11 disable sflow

Description

This command is used to disable the sFlow function on the Switch.

Format

disable sflow

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the sFlow globally:

```
DWS-3160-24PC:admin# disable sflow
Command: disable sflow

Success.

DWS-3160-24PC:admin#
```

64-12 show sflow

Description

This command is used to display the sFlow information.

Format

show sflow

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To display the sFlow information:

```
DWS-3160-24PC:admin#show sflow
Command: show sflow

 sFlow Version  : V5
 sFlow Address  : 10.90.90.90
 sFlow State    : Enabled

DWS-3160-24PC:admin#
```

64-13 show sflow flow_sampler

Description

This command is used to display the sFlow flow sampler configured for ports. The actual value rate is 256 times the displayed rate value. There are two types of rates. The Configured Rate is configured by the user. In order to limit the number of packets sent to the CPU when the rate of traffic to the CPU is high, the sampling rate will be decreased. This is specified as the active rate.

Format

show sflow flow_sampler

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To display the sFlow flow sampler information of ports which have been created:

```
DWS-3160-24PC:admin#show sflow flow_sampler
Command: show sflow flow_sampler

 Port   Analyzer Server ID   Configured Rate   Active Rate   Max Header Size
 ----   ------------------   ---------------   -----------   ---------------
 1      1                    0                 0             18

Total Entries: 1

DWS-3160-24PC:admin#
```

64-14 show sflow counter_poller

Description

This command is used to display the sFlow counter pollers which have been configured for port.

Format

show sflow counter_poller

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To display the sFlow counter poller information of ports which have been created:

```
DWS-3160-24PC:admin#show sflow counter_poller
Command: show sflow counter_poller

 Port   Analyzer Server ID   Polling Interval (sec)
 ----   ------------------   -----------------------
 1      1                    Disable

Total Entries: 1

DWS-3160-24PC:admin#
```

64-15 show sflow analyzer_server

Description

This command is used to display the sFlow analyzer server information. The Timeout field specifies the time configured by user. The Current Countdown Time is the current time remaining before the server timeout.

Format

show sflow analyzer_server

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To display the sFlow flow sampler information of ports which have been created:

```
DWS-3160-24PC:admin#show sflow analyzer_server
Command: show sflow analyzer_server

 sFlow Analyzer_server Information
 ------------------------------
 Server ID             : 1
 Owner                 : sflowowner
 Timeout               : 400
 Current Countdown Time: 361
 Collector Address     : 10.90.90.90
 Collector Port        : 6343
 Max Datagram Size     : 1400

 Server ID             : 2
 Owner                 : monitor
 Timeout               : Infinite
 Current Countdown Time: Infinite
 Collector Address     : 10.0.0.1
 Collector Port        : 65524
 Max Datagram Size     : 300

Total Entries: 2

DWS-3160-24PC:admin#
```

Chapter 65 Show Technical Support Command List

show tech_support
upload tech_support_toTFTP <ipaddr> <path_filename 64>

65-1 show tech_support

Description

This command is used by the technical support personnel to dump the device overall operation information.

Format

show tech_support

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display the information of technique’s support:

```
DWS-3160-24PC:admin# show tech_support
Command: show tech_support

#-------------------------------------------------------------------------------

#                     DWS-3160-24PC Gigabit Ethernet Switch
#                         Technical Support Information
#
#                           Firmware: Build 1.00.034
#          Copyright(C) 2012  D-Link Corporation. All rights reserved.
#-------------------------------------------------------------------------------

********************   Basic System Information   ********************

[SYS 2000-1-15 00:25:41]

Boot Time           : 14 Jan 2000  21:20:02
RTC Time            : 2000/01/15 00:25:41
Boot PROM Version   : Build 1.00.001
Firmware Version    : Build 1.00.034
Hardware Version    : A1
MAC Address         : 00-01-02-03-04-00
[ERROR_LOG 2000-1-15 00:25:41]

 Error log is empty.

********************   System Log   ********************

[SYS_LOG 2000-1-15 00:25:41]

Index Date       Time     Level   Log Text
--- ---------- -------- ------- ----------------------------------------------
16    2000-01-15 00:20:08 INFO(6) Successful Enable Admin through Console
authenticated by AAA local_enable method (Username: power)
15    2000-01-15 00:20:02 INFO(6) Successful login through Console
authenticated by AAA local method (Username:power)
14    2000-01-15 00:20:00 INFO(6) Logout through Console (Username: admin)
13    2000-01-15 00:19:59 INFO(6) Configuration saved to flash by console
(Username: admin)
12    2000-01-15 00:19:56 INFO(6) Authentication Policy is enabled (Module:
AAA)
11    2000-01-15 00:19:49 INFO(6) Successful login through Console (Username:
admin)
10    2000-01-15 00:19:47 INFO(6) Logout through Console (Username: power)
9     2000-01-15 00:19:25 INFO(6) Successful login through Console (Username:
power)
```

65-2 upload tech_support_toTFTP

Description

This command is used to upload the technical information, of this Switch, to a TFTP server.

Format

upload tech_support_toTFTP <ipaddr> <path_filename 64>

Parameters

<ipaddr> - Specifies the IP address of TFTP server.

<path_filename 64> - Specifies the file name to store the information of technique's support in TFTP server. The max size of the file name is 64.

Restrictions

Only Administrators and Operators can issue this command.

Example

To upload the technical information:

```
DWS-3160-24PC:admin# upload tech_support_to_TFTP 10.0.0.66 tech_report.txt
Command: upload tech_support_to_TFTP 10.0.0.66 tech_report.txt

 Connecting to server................... Done.
 Upload techsupport file................ Done.

 Success.

DWS-3160-24PC:admin#
```

Chapter 66 Simple Network Management Protocol (SNMP) Command List

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]

delete snmp community <community_string 32>

show snmp community {<community_string 32>}

create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}

delete snmp user <username 32>

show snmp user

create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}

delete snmp group <groupname 32>

show snmp groups

create snmp view <view_name 32> <oid> view_type [included | excluded]

delete snmp view <view_name 32> [all | <oid>]

show snmp view {<view_name 32>}

create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>

delete snmp [host <ipaddr> | v6host <ipv6addr>]

show snmp host {<ipaddr>}

show snmp v6host {<ipv6addr>}

config snmp engineID <snmp_engineID 10-64>

show snmp engineID

enable snmp

disable snmp

config snmp system_name {<sw_name>}

config snmp system_location {<sw_location>}

config snmp system_contact {<sw_contact>}

enable snmp traps

disable snmp traps

enable snmp authenticate_traps

disable snmp authenticate_traps

enable snmp linkchange_traps

disable snmp linkchange_traps

config snmp linkchange_traps ports [all | <portlist>] [enable | disable]

config snmp coldstart_traps [enable | disable]

config snmp warmstart_traps [enable | disable]

show snmp traps {linkchange_traps {ports <portlist>}}

config rmon trap {rising_alarm [enable | disable] | falling_alarm [enable | disable]} (1)

show rmon

66-1 create snmp community

Description

This command is used to create an SNMP community string.

Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the Switch. You can Specifies one or more of the following characteristics associated with the string:

An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent.

A MIB view, which defines the subset of all MIB objects accessible to the given community.

Read and write or read-only permission for the MIB objects accessible to the community.

Format

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]

Parameters

community - An alphanumeric string of up to 32 characters used to authentication of users wanting access to the Switch's SNMP agent.
<community_string> - Enter the community string value here.

view_name - Specifies to view a MIB name.
<view_name 32> - Enter the MIB view name here. This name can be up to 32 characters long.

readonly - Allows the user using the above community string to have read only access to the Switch's SNMP agent.
readwrite - Allows the user using the above community string to have read and write access to the Switch's SNMP agent. The default read only community string is public. The default read write community string is private.

Restrictions

Only Administrators can issue this command.

Example

To create a read-only level SNMP community "System" with a "CommunityView" view:

```
DWS-3160-24PC:admin# create snmp community System view CommunityView read_only
Command: create snmp community System view CommunityView read_only

Success.

DWS-3160-24PC:admin#
```

66-2 delete snmp community

Description

This command is used to delete an SNMP community string.

Format

delete snmp community <community_string 32>

Parameters

community - Community string will be deleted.

<community_string 32> - Enter the community string value here. This value can be up to 32 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a SNMP community “System”:

```
DWS-3160-24PC:admin# delete snmp community System
Command: delete snmp community System

Success.

DWS-3160-24PC:admin#
```

66-3 show snmp community

Description

This command is used to display the community string configurations.

Format

show snmp community <community_string 32>

Parameters

<community_string 32> - (Optional) Specifies the Community string.

If not Specifies community string , all community string information will be displayed.

Restrictions

None.

Example

To display SNMP community:

```
DWS-3160-24PC:admin#show snmp community
Command: show snmp community

SNMP Community Table
Community Name                    View Name                         Access
Right
--------------------------------  --------------------------------  -----------
System                            CommunityView                     read_only
private                           CommunityView                     read_write
public                            CommunityView                     read_only

Total Entries: 3

DWS-3160-24PC:admin#
```

66-4 create snmp user

Description

This command is used to create a new user to an SNMP group originated by this command.

Format

create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}

Parameters

<user_name 32> - The name of the user on the host that connects to the agent. The range is 1 to 32.

<groupname 32> - The name of the group to which the user is associated. The range is 1 to 32.

encrypted - (Optional) Specifies whether the password appears in encrypted format.

by_password - (Optional) Indicate input password for authentication and privacy.
auth - Initiates an authentication level setting session. The options are md5 and sha.
md5 - The HMAC-MD5-96 authentication level.
<auth_password 8-16> - Enter the MD5 authentication password here. This value must be between 8 and 16 characters.
sha - The HMAC-SHA-96 authentication level.
<auth_password 8-20> - Enter the SHA authentication password here. This value must be between 8 and 20 characters.

priv - (Optional) A privacy key used by DES, it is hex string type.
none - Specifies that no encryption will be used for the privacy key.
des - Specifies that the DES encryption will be used for the privacy key.
<priv_password 8-16> - Enter the DES password value here. This value must be between 8 and 16 characters long.

by_key - (Optional) Indicate input key for authentication and privacy.
auth - An authentication string used by MD5 or SHA1.
md5 - An authentication key used by MD5, it is hex string type.
<auth_key 32-32> - Enter the MD5 authentication key here. This value must be 32 characters long.
sha - An authentication key used by SHA1, it is hex string type.
<auth_key 40-40> - Enter the SHA authentication key here. This value must be 32 characters long.

priv - (Optional) A privacy key used by DES, it is hex string type.
    none - Specifies that no encryption will be used for the privacy key.
    des - Specifies that the DES encryption will be used for the privacy key.
        <priv_key 32-32> - Enter the DES privacy key here. This value must be 32 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create a SNMP user “user123” with group “group123”:

```
DWS-3160-24PC:admin# create snmp user user123 group123 encrypted by_password
auth md5 12345678 priv des 12345678
Command: create snmp user user123 group123 encrypted by_password auth md5
12345678 priv des 12345678


Success.


DWS-3160-24PC:admin#
```

66-5 delete snmp user

Description

This command is used to remove a user from an SNMP group and delete the associated group in SNMP group.

Format

delete snmp user <username 32>

Parameters

<username 32> - The name of the user on the host that connects to the agent. The range is 1 to 32.

Restrictions

Only Administrators can issue this command.

Example

To delete a SNMP user “user123”:

```
DWS-3160-24PC:admin# delete snmp user user123
Command: delete snmp user user123

Success.

DWS-3160-24PC:admin#
```

66-6 show snmp user

Description

This command is used to display information on each SNMP username in the group username table.

Format

show snmp user

Parameters

None.

Restrictions

None.

Example

To display SNMP user:

```
DWS-3160-24PC:admin#show snmp user
Command: show snmp user

Username                          Group Name                        VerAuthPriv
--------------------------------  --------------------------------  -----------
initial                           initial                           V3 NoneNone
user123                           group123                          V3 MD5 DES

Total Entries: 2

DWS-3160-24PC:admin#
```

66-7 create snmp group

Description

This command is used to create a new SNMP group, or a table that maps SNMP users to SNMP views.

Format

create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}

Parameters

group - Specifies the name of the group.

<groupname 32> - Enter the group name here. This name can be up to 32 characters long.

v1 - The least secure of the possible security models.

v2c - The second least secure of the possible security models.

v3 - The most secure of the possible.

noauth_nopriv - Neither support packet authentication nor encrypting.
auth_nopriv - Support packet authentication.
auth_priv - Support packet authentication and encrypting.

read_view - (Optional) Specifies that the view name would be read.
<view_name 32> - Enter the read view name here. This name can be up to 32 characters long.

write_view - (Optional) Specifies that the view name would be write.
<view_name 32> - Enter the write view name here. This name can be up to 32 characters long.

notify_view - (Optional) Specifies that the view name would be notify.
<view_name 32> - Enter the notify view name here. This name can be up to 32 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create SNMP group “group123”:

```
DWS-3160-24PC:admin# create snmp group group123 v3 auth_priv read_view
CommunityView write_view CommunityView notify_view CommunityView
Command: create snmp group group123 v3 auth_priv read_view CommunityView
write_view CommunityView notify_view CommunityView


Success.


DWS-3160-24PC:admin#
```

66-8 delete snmp group

Description

This command is used to remove a SNMP group.

Format

delete snmp group <groupname 32>

Parameters

<groupname 32> - The name of the group will be deleted.

Restrictions

Only Administrators can issue this command.

Example

To delete SNMP group “group123”:

```
DWS-3160-24PC:admin# delete snmp group group123
Command: delete snmp group group123

Success.

DWS-3160-24PC:admin#
```

66-9 show snmp groups

Description

This command is used to display the names of groups on the Switch and the security model, level, the status of the different views.

Format

show snmp groups

Parameters

None.

Restrictions

None.

Example

To display SNMP groups:

```
DWS-3160-24PC:admin#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

Group    Name    : System
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Securiy Model    : SNMPv1
Securiy Level    : NoAuthNoPriv

Group    Name    : System
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Securiy Model    : SNMPv2
Securiy Level    : NoAuthNoPriv

Group    Name    : public
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Securiy Model    : SNMPv1
Securiy Level    : NoAuthNoPriv
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

66-10 create snmp view

Description

This command is used to assign views to community strings to limit which MIB objects an SNMP manager can access.

Format

create snmp view <view_name 32> <oid> view_type [included | excluded]

Parameters

view - View name to be created.
  <view_name 32> - Enter the view name here. The name can be up to 32 characters long.

<oid> - Object-Identified tree, MIB tree.

view_type - Specifies the access type of the MIB tree in this view.
  included - Includes for this view.
  excluded - Excluded for this view.

Restrictions

Only Administrators can issue this command.

Example

To create SNMP view “view123”:

```
DWS-3160-24PC:admin# create snmp view view123 1.3.6 view_type included
Command: create snmp view view123 1.3.6 view_type included

Success.

DWS-3160-24PC:admin#
```

66-11 delete snmp view

Description

This command is used to remove a view record.

Format

delete snmp view <view_name 32> [all | <oid>]

Parameters

view - View name to be deleted. **<view_name 32>** - Enter the view name here. The name can be up to 32 characters long.
all - Specifies that all view records will be removed. **<oid>** - Object-Identified tree, MIB tree.

Restrictions

Only Administrators can issue this command.

Example

To delete SNMP view “view123”:

```
DWS-3160-24PC:admin# delete snmp view view123 all
Command: delete snmp view view123 all

Success.

DWS-3160-24PC:admin#
```

66-12 show snmp view

Description

This command is used to display the SNMP view record.

Format

show snmp view {<view_name 32>}

Parameters

view - (Optional) View name of the user who likes to display.
<view_name 32> - Enter the view name here. The name can be up to 32 characters long.

Restrictions

None.

Example

To display SNMP view:

```
DWS-3160-24PC:admin#show snmp view
Command: show snmp view

Vacm View Table Settings
View Name                         Subtree                             View Type
--------------------------------  ----------------------------------  ---------
-
view123                           1.3.6                               Included
restricted                        1.3.6.1.2.1.1                       Included
restricted                        1.3.6.1.2.1.11                      Included
restricted                        1.3.6.1.6.3.10.2.1                  Included
restricted                        1.3.6.1.6.3.11.2.1                  Included
restricted                        1.3.6.1.6.3.15.1.1                  Included
CommunityView                     1                                   Included
CommunityView                     1.3.6.1.6.3                         Excluded
CommunityView                     1.3.6.1.6.3.1                       Included

Total Entries: 9

DWS-3160-24PC:admin#
```

66-13 create snmp

Description

This command is used to create a recipient of an SNMP trap operation.

Format

create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>

Parameters

host - Specifies the recipient for which the traps are targeted.
<ipaddr> - The IP address of the recipient for which the traps are targeted.

v6host - Specifies the IPv6 host address to which the trap packet will be sent.
<ipv6addr> - The IPv6 address of the recipient for which the traps are targeted.

v1 - The least secure of the possible security models.
v2c - The second least secure of the possible security models.
v3 - The most secure of the possible.

noauth_nopriv - Neither support packet authentication nor encrypting.
auth_nopriv - Support packet authentication.
auth_priv - Support packet authentication and encrypting.
<auth_string 32> - Authentication string. If the v1 or v2 is specified, the auth_string presents the community string, and it must be one of the entries in community table. If the v3 is specified, the auth_string presents the user name, and it must be one of the entries in the user table.

Restrictions

Only Administrators can issue this command.

Example

To create SNMP host “10.0.0.1” with community string “public”:

```
DWS-3160-24PC:admin# create snmp host 10.0.0.1 v1 public
Command: create snmp host 10.0.0.1 v1 public

Success.

DWS-3160-24PC:admin#
```

66-14 delete snmp

Description

This command is used to delete a recipient of an SNMP trap operation.

Format

delete snmp [host <ipaddr> | v6host <ipv6addr>]

Parameters

host - The IP address of the recipient for which the traps are targeted.
<ipaddr> - Enter the IP address used for the configuration here.

v6host - The IPv6 address of the recipient for which the traps are targeted.
<ipv6addr> - Enter the IPv6 address used for the configuration here.

Restrictions

Only Administrators can issue this command.

Example

To delete SNMP host “10.0.0.1”:

```
DWS-3160-24PC:admin# delete snmp host 10.0.0.1
Command: delete snmp host 10.0.0.1

Success.

DWS-3160-24PC:admin#
```

66-15 show snmp host

Description

This command is used to display the recipient for which the traps are targeted.

Format

show snmp host {<ipaddr>}

Parameters

host - (Optional) The IP address of the recipient for which the traps are targeted.
 <ipaddr> - Enter the IP address used for the configuration here.

If no parameter specified, all SNMP hosts will be displayed.

Restrictions

None.

Example

To display SNMP host(s):

```
DWS-3160-24PC:admin#show snmp host
Command: show snmp host

SNMP Host Table
Host IP Address  SNMP Version     Community Name / SNMPv3 User Name
---------------  ---------------  ---------------------------------
10.0.0.1         V1               public

Total Entries: 1

DWS-3160-24PC:admin#
```

66-16 show snmp v6host

Description

This command is used to display the recipient for which the traps are targeted.

Format

show snmp v6host {<ipv6addr>}

Parameters

v6host - (Optional) Specifies the IPv6 host address. **<ipv6addr>** - Enter the IPv6 address used for the configuration here.
If no parameter specified, all SNMP hosts will be displayed.

Restrictions

None.

Example

To display SNMP host:

```
DWS-3160-24PC:admin# show snmp v6host
Command: show snmp v6host

SNMP Host Table
------------------------------------------------------------------
Host IPv6 Address : 3FFE::3
SNMP Version      : V3 na/np
Community Name/SNMPv3 User Name : initial

Host IPv6 Address : 3FFE::2
SNMP Version      : V2c
Community Name/SNMPv3 User Name : private

Host IPv6 Address : 3FFE::1
SNMP Version      : V1
Community Name/SNMPv3 User Name : public

Host IPv6 Address : 3FFE::3
SNMP Version      : V3  a/np
Community Name/SNMPv3 User Name : user123

Host IPv6 Address : 3FFE::3
SNMP Version      : V3  a/ p
Community Name/SNMPv3 User Name : user234

Total Entries: 5

DWS-3160-24PC:admin#
```

66-17 config snmp engineID

Description

This command is used to configure a identifier for the SNMP engine on the Switch.

Format

config snmp engineID <snmp_engineID 10-64>

Parameters

engineID - Identify for the SNMP engine on the Switch. It is octet string type. It accepts the hex number directly.

<snmp_engineID 10-64> - Enter the SNMP engine ID here. This value must be between 10 and 64.

Restrictions

Only Administrators can issue this command.

Example

To configure SNMP engine ID to “1023457890”:

```
DWS-3160-24PC:admin# config snmp engineID 1023457890
Command: config snmp engineID 1023457890

Success.

DWS-3160-24PC:admin#
```

66-18 show snmp engineID

Description

This command is used to display the identification of the SNMP engine on the Switch. The default value is suggested in RFC2271. The very first bit is 1, and the first four octets are set to the binary equivalent of the agent’s SNMP management private enterprise number as assigned by IANA, D-Link is 171. The fifth octet is 03 to indicate the rest is the MAC address of this device. The 6th – 11th octets is MAC address.

Format

show snmp engineID

Parameters

None.

Restrictions

None.

Example

To display the SNMP engine ID:

```
DWS-3160-24PC:admin#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 1023457890

DWS-3160-24PC:admin#
```

66-19 enable snmp

Description

This command is used to enable the SNMP function.

Format

enable snmp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable SNMP:

```
DWS-3160-24PC:admin# enable snmp
Command: enable snmp

Success.

DWS-3160-24PC:admin#
```

66-20 disable snmp

Description

This command is used to disable the SNMP function.

Format

disable snmp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable SNMP:

```
DWS-3160-24PC:admin# disable snmp
Command: disable snmp

Success.

DWS-3160-24PC:admin#
```

66-21 config snmp system_name

Description

This command is used to configure the name for the Switch.

Format

config snmp system_name {<sw_name>}

Parameters

system_name - A maximum of 128 characters is allowed. And NULL string is accepted.
<sw_name> - (Optional) Enter the system name used here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the Switch name for “Technical”:

```
DWS-3160-24PC:admin#config snmp system_name Technical
Command: config snmp system_name Technical

Success.

DWS-3160-24PC:admin#
```

66-22 config snmp system_location

Description

This command is used to enter a description of the location of the Switch.

Format

config snmp system_location {<sw_location>}

Parameters

system_location - A maximum of 128 characters is allowed. And NULL string is accepted

<sw_location> - (Optional) Enter the system location string here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the Switch location for “HQ 5F”:

```
DWS-3160-24PC:admin# config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DWS-3160-24PC:admin#
```

66-23 config snmp system_contact

Description

This command is used to enter the name of a contact person who is responsible for the Switch.

Format

config snmp system_contact {<sw_contact>}

Parameters

system_contact - A maximum of 128 characters is allowed. And NULL string is accepted.

<sw_contact> - (Optional) Enter the system contact string here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the Switch contact to “MIS Department II”:

```
DWS-3160-24PC:admin# config snmp system_contact "MIS Department II"
Command: config snmp system_contact "MIS Department II"

Success.

DWS-3160-24PC:admin#
```

66-24 enable snmp traps

Description

This command is used to enable SNMP trap support.

Format

enable snmp traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable SNMP trap support:

```
DWS-3160-24PC:admin# enable snmp traps
Command: enable snmp traps

Success.

DWS-3160-24PC:admin#
```

66-25 disable snmp traps

Description

This command is used to disable SNMP trap support on the Switch.

Format

disable snmp traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To prevent SNMP traps from being sent from the Switch:

```
DWS-3160-24PC:admin# disable snmp traps
Command: disable snmp traps

Success.

DWS-3160-24PC:admin#
```

66-26 enable snmp authenticate_traps

Description

This command is used to enable SNMP authentication failure trap support.

Format

enable snmp authenticate_traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable SNMP authentication trap support:

```
DWS-3160-24PC:admin# enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

DWS-3160-24PC:admin#
```

66-27 disable snmp authenticate_traps

Description

This command is used to disable SNMP authentication failure trap support.

Format

disable snmp authenticate_traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable SNMP authentication trap support:

```
DWS-3160-24PC:admin# disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

DWS-3160-24PC:admin#
```

66-28 enable snmp linkchange_traps

Description

This command is used to configure the sending of link change traps.

Format

enable snmp linkchange_traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the sending of link change traps:

```
DWS-3160-24PC:admin# enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

DWS-3160-24PC:admin#
```

66-29 disable snmp linkchange_traps

Description

This command is used to configure the sending of link change traps.

Format

disable snmp linkchange_traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the sending of link change traps:

```
DWS-3160-24PC:admin# disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

DWS-3160-24PC:admin#
```

66-30 config snmp linkchange_traps ports

Description

This command is used to configure the sending of link change traps and per port control for sending of change trap.

Format

config snmp linkchange_traps ports [all | <portlist>] [enable | disable]

Parameters

all - Specifies all ports.
<portlist> - Specifies a port range.

enable - Enable sending of the link change trap for this port.
disable - Disable sending of the link change trap for this port.

Restrictions

Only Administrators can issue this command.

Example

To configure the sending of link change traps:

```
DWS-3160-24PC:admin# config snmp linkchange_traps ports 1-4 enable
Command: config snmp linkchange_traps ports 1-4 enable

Success.

DWS-3160-24PC:admin#
```

66-31 config snmp coldstart_traps

Description

This command is used to configure the trap for cold start event.

Format

config snmp coldstart_traps [enable | disable]

Parameters

enable - Enable the trap of the cold start event. The default state is enabled.
disable - Disable the trap of the cold start event.

Restrictions

Only Administrators can issue this command.

Example

To configure the trap for cold start event:

```
DWS-3160-24PC:admin# config snmp coldstart_traps enable
Command: config snmp coldstart_traps enable

Success.

DWS-3160-24PC:admin#
```

66-32 config snmp warmstart_traps

Description

This command is used to configure the trap state for warm start event.

Format

config snmp warmstart_traps [enable | disable]

Parameters

enable - Enable the trap of the warm start event. The default state is enabled.
disable - Disable the trap of the warm start event.

Restrictions

Only Administrators can issue this command.

Example

To configure the trap state for warm start event:

```
DWS-3160-24PC:admin# config snmp warmstart_traps enable
Command: config snmp warmstart_traps enable

Success.

DWS-3160-24PC:admin#
```

66-33 show snmp traps

Description

This command is used to display the SNMP trap sending status.

Format

show snmp traps {linkchange_traps {ports <portlist>}}

Parameters

linkchange_traps - (Optional) Specifies that the SNMP trap sending status will be displayed.

ports - (Optional) Specifies the ports for the display.
<portlist> - Enter the list of ports used for the display here.

Restrictions

None.

Example

To display the SNMP traps information:

```
DWS-3160-24PC:admin#show snmp traps
Command: show snmp traps

SNMP Traps         : Enabled
Authenticate Trap  : Enabled
Linkchange Traps   : Enabled
Coldstart Traps    : Enabled
Warmstart Traps    : Enabled

DWS-3160-24PC:admin#
```

66-34 config rmon trap

Description

This command is used to configure the trap state for RMON events.

Format

config rmon trap {rising_alarm [enable | disable] | falling_alarm [enable | disable]} (1)

Parameters

rising_alarm - (Optional) Specifies the trap state for rising alarm. The default state is enabled.
- **enable** - Specifies that the rising alarm function will be enabled.
- **disable** - Specifies that the rising alarm function will be disabled.

falling_alarm - (Optional) Specifies the trap state for falling alarm. The default state is enabled.
- **enable** - Specifies that the falling alarm function will be enabled.
- **disable** - Specifies that the falling alarm function will be disabled.

Restrictions

Only Administrators can issue this command.

Example

To configure the trap state for RMON events:

```
DWS-3160-24PC:admin# config rmon trap rising_alarm disable
Command: config rmon trap rising_alarm disable

Success.

DWS-3160-24PC:admin#
```

66-35 show rmon

Description

This command is used to display the RMON related setting.

Format

show rmon

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display the RMON related setting:

```
DWS-3160-24PC:admin#show rmon
Command: show rmon

RMON Rising Alarm Trap      : Disabled
RMON Falling Alarm Trap     : Enabled

DWS-3160-24PC:admin#
```

Chapter 67 Single IP Management Command List

enable sim

disable sim

show sim {[candidates {<candidate_id 1-100>} | members {<member_id 1-4>} | group {commander_mac <macaddr>} | neighbor]}

reconfig [member_id <value 1-4> | exit]

config sim_group [add <candidate_id 1-100> {<password>} | delete <member_id 1-4>]

config sim [{[commander {group_name <groupname 64>} | candidate] | dp_interval <sec 30-90> | hold_time <sec 100-255>}]

download sim_ms [firmware_from_tftp | configuration_from_tftp] <ipaddr> <path_filename> {[members <mslist 1-4> | all]}

upload sim_ms [configuration_to_tftp | log_to_tftp] <ipaddr> <path_filename> [members <mslist> | all]

67-1 enable sim

Description

This command is used to enable the Single IP Management (SIM) feature on the Switch.

Format

enable sim

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable SIM:

```
DWS-3160-24PC:admin# enable sim
Command: enable sim

Success.

DWS-3160-24PC:admin#
```

67-2 disable sim

Description

This command is used to disable the SIM feature on the Switch.

Format

disable sim

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable SIM:

```
DWS-3160-24PC:admin# disable sim
Command: disable sim

Success.

DWS-3160-24PC:admin#
```

67-3 show sim

Description

This command is used to display the current information of the specific sort of devices.

Format

show sim {[candidates {<candidate_id 1-100>} | members {<member_id 1-4>} | group {commander_mac <macaddr>} | neighbor]}

Parameters

candidates - (Optional) Specifies the candidate devices.
  <candidate_id 1-100> - Enter the candidate device ID here. This value must be between 1 and 100.

members - (Optional) Specifies the member devices.
  <member_id 1-4> - Enter the member device ID here. This value must be between 1 and 4.

group - (Optional) Specifies other group devices.
  commander_mac - Specifies the commander MAC address used.
    <macaddr> - Enter the commander MAC address used here.

neighbor - (Optional) Specifies other neighbor devices.

Restrictions

None.

Example

To display the self information in detail:

```
DWS-3160-24PC:admin#show sim
Command: show sim

Group Name         : Internal
SIM Version        : VER-1.61
Firmware Version   : 1.00.034
Device Name        :
MAC Address        : 00-11-22-33-45-67
Capabilities       : L2
Platform           : DWS-3160-24PC L2 Switch
SIM State          : Enabled
Role State         : Commander
Discovery Interval : 30 sec
Hold Time          : 100 sec

DWS-3160-24PC:admin#
```

To display the candidate information in summary, if user Specifies candidate id, it would display information in detail:

```
DWS-3160-24PC:admin#show sim candidates
Command: show sim candidates

ID  MAC Address       Platform /               Hold  Firmware  Device Name
                      Capability               Time  Version
--- ----------------- ------------------------ ----- --------- ----------------
 1  00-11-22-33-32-32 DWS-3160-24TC L2 Switch  80    1.00.034

Total Entries: 1

DWS-3160-24PC:admin#
```

To display the member information in summary, if user Specifies member id, it will display information in detail:

```
DWS-3160-24PC:admin#show sim member
Command: show sim members

ID  MAC Address       Platform /               Hold  Firmware  Device Name
                      Capability               Time  Version
--- ----------------- ------------------------ ----- --------- ----------------
 1  00-11-22-33-32-32 DWS-3160-24TC L2 Switch  80    1.00.034

Total Entries: 1

DWS-3160-24PC:admin#
```

To display the group information in detail:

```
DWS-3160-24PC:admin#show sim group commander_mac 00-11-22-33-45-67
Command: show sim group commander_mac 00-11-22-33-45-67

== Group Info Table ==

[*** Commander Info ***]

MAC Address           : 00-11-22-33-45-67
Group Name            : Internal
Device Name           :
Firmware Version      : 1.00.034
Capabilities          : L2
Platform              : DWS-3160-24PC L2 Switch
No. of Members        : 1
Hold Time             : --
        [*** Member Info (1/1)***]

        MAC Address    : 00-11-22-33-32-32

DWS-3160-24PC:admin#
```

To display neighbor table of SIM:

```
DWS-3160-24PC:admin#show sim neighbor
Command: show sim neighbor

Neighbor Info Table

Port   MAC Address        Role
------ ----------------- ---------
23     00-11-22-33-32-32  Member

Total Entries: 1

DWS-3160-24PC:admin#
```

67-4 reconfig

Description

This command is used to reconnect to a SIM member, by using the member ID.

Format

reconfig [member_id <value 1-4> | exit]

Parameters

member_id - (Optional) Specifies the serial number of the member.
<value 1-4> - Enter the serial number ID of the member here.

exit - (Optional) Specifies to exit from the TELNET session.

Restrictions

Only Administrators can issue this command.

Example

To reconnect to a member:

```
DWS-3160-24PC:admin# reconfig member_id 1
Command: reconfig member_id 1

DWS-3160-24PC:admin#
Login:
```

67-5 config sim_group

Description

This command is used to configure SIM group information.

Format

config sim_group [add <candidate_id 1-100> {<password>} | delete <member_id 1-4>]

Parameters

add - Specifies to add a specific candidate to the group.
<candidate_id 1-100> - Enter the candidate ID to be added to the group here. This value must be between 1 and 100.

<password> - (Optional) The password of candidate if necessary.

delete - Specifies to delete a member from the group.
<member_id 1-4> - Enter the member ID of the member to be removed from the group here. This value must be between 1 and 4.

Restrictions

Only Administrators can issue this command.

Example

To add a member:

```
DWS-3160-24PC:admin# config sim_group add 2
Command: config sim_group add 2

Please wait for ACK !!!
SIM Configure Success !!!

Success.

DWS-3160-24PC:admin#
```

To delete a member:

```
DWS-3160-24PC:admin# config sim_group delete 1
Command: config sim_group delete 1

Please wait for ACK !!!
SIM Configure Success !!!

Success.

DWS-3160-24PC:admin#
```

67-6 config sim

Description

This command is used to configure the role state and the parameters of the discovery protocol on the Switch.

Format

config sim [{[commander {group_name <groupname 64>} | candidate] | dp_interval <sec 30-90> | hold_time <sec 100-255>}]

Parameters

commander - (Optional) Specifies to transfer the role to the commander.

group_name - (Optional) Specifies that if the user is the commander, the user can update the name of group.
<groupname 64> - Enter the group name here. This name can be up to 64 characters long.

candidate - (Optional) Specifies to transfer the role to the candidate.

dp_interval - (Optional) The time in seconds between discoveries.
<sec 30-90> - Enter the discovery time here in seconds. This value must be between 30 and 90 seconds.

hold_time - (Optional) The time in seconds the device holds the discovery result.
<sec 100-255> - Enter the hold time here in seconds. This value must be between 100 and 255.

Restrictions

Only Administrators can issue this command.

Example

To transfer to commander:

```
DWS-3160-24PC:admin# config sim commander
Command: config sim commander

Success.

DWS-3160-24PC:admin#
```

To transfer to candidate:

```
DWS-3160-24PC:admin# config sim candidate
Command: config sim candidate

Success.

DWS-3160-24PC:admin#
```

To update name of group:

```
DWS-3160-24PC:admin# config sim commander group_name mygroup
Command: config sim commander group_name mygroup

Success.

DWS-3160-24PC:admin#
```

To change the time interval of discovery protocol:

```
DWS-3160-24PC:admin# config sim dp_interval 30
Command: config sim dp_interval 30

Success.

DWS-3160-24PC:admin#
```

To change the hold time of discovery protocol:

```
DWS-3160-24PC:admin# config sim hold_time 200
Command: config sim hold_time 200

Success.

DWS-3160-24PC:admin#
```

67-7 download sim_ms

Description

This command is used to download firmware or a configuration to a specific device.

Format

download sim_ms [firmware_from_tftp | configuration_from_tftp] <ipaddr> <path_filename> {[members <mslist 1-4> | all]}

Parameters

firmware_from_tftp - Specifies that the firmware will be downloaded from the TFTP server.

configuration_from_tftp - Specifies that the configuration will be downloaded from the TFTP server.

<ipaddr> - Specifies the IP address of the TFTP server.

<path_filename> - Specifies the file path of the firmware or configuration in the TFTP server.

members – (Optional) Specifies a range of members who can download this firmware or configuration.
<mslist 1-4> - Enter the member list used here. This value must be between 1 and 4.
all - Specifies that all members will be used.

Restrictions

Only Administrators can issue this command.

Example

To download the configuration:

```
DWS-3160-24PC:admin# download sim_ms configuration_from_tftp 10.55.47.1
D:\dwl600x.tfp members 1
Commands: download sim_ms configuration_from_tftp 10.55.47.1 D:\dwl600x.tfp
members 1

This device is updating configuration. Please wait several minutes ...

Download Status :

ID   MAC Address        Result
---  -----------------  ----------------
1   00-01-02-03-04-00  Success

DWS-3160-24PC:admin#
```

To download the firmware:

```
DWS-3160-24PC:admin# download sim_ms firmware_from_tftp 10.55.47.1 D:\test.txt
members 1
Commands: download sim_ms firmware_from_tftp 10.55.47.1 D:\test.txt members 1

This device is updating firmware. Please wait several minutes ...

Download Status :

ID   MAC Address        Result
---  -----------------  ----------------
1   00-01-02-03-04-00  Success

DWS-3160-24PC:admin#
```

67-8 upload sim_ms

Description

This command is used to upload a configuration to the TFTP server.

Format

upload sim_ms [configuration_to_tftp | log_to_tftp] <ipaddr> <path_filename> [members <mslist> | all]

Parameters

configuration_to_tftp - Specifies that the configuration will be uploaded to the TFTP server.

log_to_tftp – Specifies that the log file will be uploaded to the TFTP server.

<ipaddr> - Specifies the IP address of the TFTP server.

<path_filename> - Specifies the file path to store the configuration in the TFTP server.

members - Specifies a range of members who can up this configuration.
- **<mslist>** - Enter the member list used here.
- **all** - Specifies that all members will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To upload the configuration:

```
DWS-3160-24PC:admin# upload sim_ms configuration_to_tftp 10.55.47.1
D:\configuration.txt members 1
Command: upload sim_ms configuration_to_tftp 10.55.47.1 D:\configuration.txt
members 1


This device is uploading configuration. Please wait several minutes ...


Upload Status :


ID   MAC Address       Result
---  ----------------- ----------------
 1   00-1A-2D-00-12-12 Transfer Fail


DWS-3160-24PC:admin#
```

Chapter 68 Syslog and Trap Source-interface Command List

config syslog source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]

show syslog source_ipif

config trap source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr> } | none]

show trap source_ipif

68-1 config syslog source_ipif

Description

This command is used to configure the syslog source IP interface.

Format

config syslog source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]

Parameters

ipif - Specifies the IP interface name. If only Specifies this parameter, the least IPv4 address and the smallest IPv6 address of ipif_name will be used as source IP addresses.

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.

<ipaddr> - (Optional) Enter the IP address used for the configuration here.

<ipv6addr> - (Optional) Enter the IPv6 address used for the configuration here.

none - Specifies to clear the configured source IP interface.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the syslog source IP interface:

```
DWS-3160-24PC:admin#config syslog source_ipif System 10.90.90.90
Command: config syslog source_ipif System 10.90.90.90

Success.

DWS-3160-24PC:admin#
```

To clear the configured source IP interface for syslog:

```
DWS-3160-24PC:admin# config syslog source_ipif none
Command: config syslog source_ipif none

Success

DWS-3160-24PC:admin#
```

68-2 show syslog source_ipif

Description

This command is used to display the syslog source IP interface.

Format

show syslog source_ipif

Parameters

None.

Restrictions

None.

Example

To display the syslog source IP interface:

```
DWS-3160-24PC:admin#show syslog source_ipif
Command: show syslog source_ipif

 Syslog Source IP Interface Configuration:

 IP Interface           : System
 IPv4 Address           : 10.90.90.90
 IPv6 Address           : None

DWS-3160-24PC:admin#
```

68-3 config trap source_ipif

Description

This command is used to configure the trap source IP interface.

Format

config trap source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr> } | none]

Parameters

ipif - Specifies the IP interface name. If only Specifies this parameter, the least IPv4 address and the smallest IPv6 address of ipif_name will be used as source IP addresses.
<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
<ipaddr> - (Optional) Enter the IP address used for the configuration here.
<ipv6addr> - (Optional) Enter the IPv6 address used for the configuration here.
none - Specifies to clear the configured source IP interface.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the trap source IP interface:

```
DWS-3160-24PC:admin# config trap source_ipif System
Command: config trap source_ipif System

Success

DWS-3160-24PC:admin#
```

To clear the configured trap source IP interface:

```
DWS-3160-24PC:admin# config trap source_ipif none
Command: config trap source_ipif none

Success

DWS-3160-24PC:admin#
```

68-4 show trap source_ipif

Description

This command is used to display the trap source IP interface.

Format

show trap source_ipif

Parameters

None.

Restrictions

None.

Example

To display the trap source IP interface:

```
DWS-3160-24PC:admin#show trap source_ip
Command: show trap source_ipif

 Trap Source IP Interface Configuration:

 IP Interface           : System
 IPv4 Address           : None
 IPv6 Address           : None

DWS-3160-24PC:admin#
```

Chapter 69 System Log Command List

clear log

show log {[index <value_list> | severity {module <module_list>} {emergency | alert | critical | error | warning | notice | informational | debug | <level_list 0-7>} | module<module_list>]}

show log_software_module

enable syslog

disable syslog

show syslog

config syslog host [<index> | all] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress [<ipaddr> | <ipv6addr>] | state [enable | disable]}

create syslog host <index 1-4> ipaddress [<ipaddr> | <ipv6addr>] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]}

delete syslog host [<index 1-4> | all]

show syslog host {<index 1-4>}

config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]

show log_save_timing

show attack_log {index <value_list>}

clear attack_log

69-1 clear log

Description

This command is used to clear the Switch’s history log.

Format

clear log

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the Switch’s history log:

```
DWS-3160-24PC:admin# clear log
Command: clear log

Success.

DWS-3160-24PC:admin#
```

69-2 show log

Description

This command is used to display the Switch's history log.

Format

show log {[index <value_list> | severity {module <module_list>} {emergency | alert | critical | error | warning | notice | informational | debug | <level_list 0-7>} | module<module_list>]}

Parameters

index - (Optional) Specifies to enter the index number of the entry to display here.
<value_list> - Enter the index number of the entry to display here.

severity - (Optional) Specifies the severity level used.

module - (Optional) Specifies the modules which are to be displayed. The module can be obtained by using the 'show log_support_module' command. Use a comma to separate multiple modules.
<module_list> - Enter the module list value here.

emergency - (Optional) Severity level 0
alert - (Optional) Severity level 1
critical - (Optional) Severity level 2
error - (Optional) Severity level 3
warning - (Optional) Severity level 4
notice - (Optional) Severity level 5
informational - (Optional) Severity level 6
debug - (Optional) Severity level 7
<level_list 0-7> - Specifies a list of severity level which is to be displayed. If there is more than one severity level, please separate them by comma. The level number is from 0 to 7.

module - (Optional) Specifies the modules which are to be displayed. The module can be obtained by using the show log_support_module command. Use a comma to separate multiple modules.
<module_list> - Enter the module list value here.

If no parameter is specified, all history log entries will be displayed.

Restrictions

None.

Example

To display the Switch's history log:

```
DWS-3160-24PC:admin#show log index 1-3
Command: show log index 1-3

Index Date       Time     Level   Log Text
----- ---------- -------- ------- -------------------------------------------
-

3     2000-01-29 03:42:35 CRIT(2) System started up
2     2000-01-29 03:42:35 CRIT(2) System cold start
1     2000-01-29 03:41:43 INFO(6) Port 2 link down

DWS-3160-24PC:admin#
```

69-3 show log_software_module

Description

This command is used to display the protocols or applications that support the enhanced log. The enhanced log adds the module name and module ID. Network administrators can display logs by module name or module ID.

Format

show log_software_module

Parameters

None.

Restrictions

None.

Example

To display the protocols or applications that support the enhanced log:

```
DWS-3160-24PC:admin#show log_software_module
Command: show log_software_module

CFM_EXT             CP                  ERPS                ERROR_LOG
MSTP                VRRP                WLAN

DWS-3160-24PC:admin#
```

69-4 enable syslog

Description

This command is used to enable the sending of syslog messages.

Format

enable syslog

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the sending of syslog messages:

```
DWS-3160-24PC:admin# enable syslog
Command: enable syslog

Success.

DWS-3160-24PC:admin#
```

69-5 disable syslog

Description

This command is used to disable the sending of syslog messages.

Format

disable syslog

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the sending of syslog messages:

```
DWS-3160-24PC:admin# disable syslog
Command: disable syslog

Success.

DWS-3160-24PC:admin#
```

69-6 show syslog

Description

This command is used to display the syslog protocol global state.

Format

show syslog

Parameters

None.

Restrictions

None.

Example

To display the syslog protocol global state:

```
DWS-3160-24PC:admin#show syslog
Command: show syslog

Syslog Global State: Enabled

DWS-3160-24PC:admin#
```

69-7 config syslog host

Description

This command is used to configure the syslog host configurations. The user can choose and report a specific level of messages to a specific host. When the user chooses a specific level for a specific host, messages which are at that severity level or higher will be reported to the specified host.

Format

config syslog host [<index> | all] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress [<ipaddr> | <ipv6addr>] | state [enable | disable]}

Parameters

host - The host index or all hosts.

  <index> - Enter the host index value here.

  all - Specifies that all the host indexes will be used.

severity - (Optional) Specifies the severity level.

  emergency - Severity level 0

alert - Severity level 1
critical - Severity level 2
error - Severity level 3
warning - Severity level 4
notice - Severity level 5
informational - Severity level 6
debug - Severity level 7
<level 0-7> - Enter the severity level value here. This value must be between 0 and 7.

facility - (Optional) 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 displayed below. This facility setting will be put in the syslog packet when it is sent to a specific syslog server.
local0 - Specifies that the user-defined facility will be set to local 0.
local1 - Specifies that the user-defined facility will be set to local 1.
local2 - Specifies that the user-defined facility will be set to local 2.
local3 - Specifies that the user-defined facility will be set to local 3.
local4 - Specifies that the user-defined facility will be set to local 4.
local5 - Specifies that the user-defined facility will be set to local 5.
local6 - Specifies that the user-defined facility will be set to local 6.
local7 - Specifies that the user-defined facility will be set to local 7.

udp_port - (Optional) Specifies the UDP port number.
<udp_port_number> - Enter the UDP port number used here.

ipaddress - (Optional) Specifies IP address for the host.
<ipaddr> - Enter the IP address used for the configuration here.
<ipv6addr> - Enter the IPv6 address used for the configuration here.

state - (Optional) The syslog protocol is used for the transmission of event notification messages across networks to a host. The option enables or disables the host to receive such messages.
enable - Specifies that the host to receive such messages will be enabled.
disable - Specifies that the host to receive such messages will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the syslog host configuration:

```
DWS-3160-24PC:admin# config syslog host all severity debug facility local0
Command: config syslog host all severity debug facility local0

Success.

DWS-3160-24PC:admin#
```

69-8 create syslog host

Description

This command is used to create a new syslog host. The user can choose and report specific levels of messages to a specific host. When the user chooses a specific level for a specific host, messages which are at that severity level or higher will be reported to that host.

Format

create syslog host <index 1-4> ipaddress [<ipaddr> |<ipv6addr>] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]}

Parameters

host - The host index or all hosts.
<index> - Enter the host index value here.
all - Specifies that all the host indexes will be used.

severity - (Optional) Specifies the severity level.
emergency - Severity level 0
alert - Severity level 1
critical - Severity level 2
error - Severity level 3
warning - Severity level 4
notice - Severity level 5
informational - Severity level 6
debug - Severity level 7
<level 0-7> - Enter the severity level value here. This value must be between 0 and 7.

facility - (Optional) 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 displayed below. This facility setting will be put in the syslog packet when it is sent to a specific syslog server.
local0 - Specifies that the user-defined facility will be set to local 0.
local1 - Specifies that the user-defined facility will be set to local 1.
local2 - Specifies that the user-defined facility will be set to local 2.
local3 - Specifies that the user-defined facility will be set to local 3.
local4 - Specifies that the user-defined facility will be set to local 4.
local5 - Specifies that the user-defined facility will be set to local 5.
local6 - Specifies that the user-defined facility will be set to local 6.
local7 - Specifies that the user-defined facility will be set to local 7.

udp_port - (Optional) Specifies the UDP port number.
<udp_port_number> - Enter the UDP port number used here.

ipaddress - (Optional) Specifies IP address for the host.
<ipaddr> - Enter the IP address used for the configuration here.
<ipv6addr> - Enter the IPv6 address used for the configuration here.

state - (Optional) The syslog protocol is used for the transmission of event notification messages across networks to a host. The option enables or disables the host to receive such messages.
enable - Specifies that the host to receive such messages will be enabled.
disable - Specifies that the host to receive such messages will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a new syslog host:

```
DWS-3160-24PC:admin# create syslog host 1 ipaddress 10.90.90.1 severity all
debug facility local0
Command: create syslog host 1 ipaddress 10.90.90.1 severity all debug facility
local0

Success.

DWS-3160-24PC:admin#
```

69-9 delete syslog host

Description

This command is used to delete a syslog host(s).

Format

delete syslog host [<index 1-4> | all]

Parameters

host - The host index or all hosts.
  <index> - Enter the host index value here.
  all - Specifies that all the host indexes will be used.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the specific syslog host:

```
DWS-3160-24PC:admin# delete syslog host 4
Command: delete syslog host 4

Success.

DWS-3160-24PC:admin#
```

69-10 show syslog host

Description

This command is used to display the syslog host configurations.

Format

show syslog host {<index 1-4>}

Parameters

host - The host index or all hosts. **<index>** - (Optional) Enter the host index value here.
If no parameter is specified, all hosts will be displayed.

Restrictions

None.

Example

To display the syslog host information:

```
DWS-3160-24PC:admin# show syslog host
Command: show syslog host

Syslog Global State: Enabled

Host  1
  IP Address        : 10.90.90.1
  Severity          : Debug(7)
  Facility          : Local0
  UDP Port          : 514
  Status            : Disabled

Host  2
  IP Address        : 3000:501:100:ffff:101:202:303:1
  Severity          : Emergency
  Facility          : Local0
  UDP port          : 514
  Status            : Disabled

Host  3
  IP Address        : 10.21.13.1
  Severity          : All
  Facility          : Local0
  UDP port          : 514
  Status            : Disabled

Total Entries : 3

DWS-3160-24PC:admin#
```

69-11 config log_save_timing

Description

This command is used to configure the method for saving the log.

Format

config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]

Parameters

time_interval – Specifies the interval used to save the log to the flash. (If no new log events occur in this period, don't save.)

<min 1-65535> - Enter the time interval value here. This value must be between 1 and 65535 minutes.

on_demand - Save log to flash whenever the user enters the "save log" or "save all" command. The default setting is on_demand.

log_trigger - Save log to flash whenever a new log event arrives.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the method for saving a log as on demand:

```
DWS-3160-24PC:admin# config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.

DWS-3160-24PC:admin#
```

69-12 show log_save_timing

Description

This command is used to display the method for saving the log.

Format

show log_save_timing

Parameters

None.

Restrictions

None.

Example

To display the timing method used for saving the log:

```
DWS-3160-24PC:admin#show log_save_timing
Command: show log_save_timing

Saving Log Method: On_demand

DWS-3160-24PC:admin#
```

69-13 show attack_log

Description

This command is used to display attack log messages. The attack log message refers to log messages driven by modules such as DOS and the IP-MAC-port binding module. This type of log message may generate a large amount of messages and quickly cause the system to run out of system log storage. Therefore, for this type of log messages only the first log that is generated each minute can be stored in the system log, with the rest of them being stored in a separate table named attack log.

Format

show attack_log {index <value_list>}

Parameters

index - (Optional) The list of index numbers of the entries that need to be displayed. For example, show attack_log index 1-5 will display the attack log messages from 1 to 5. **<value_list>** - Enter the index numbers of the entries that needs to be displayed here.
If no parameter is specified, all entries in the attack log will be displayed.

Restrictions

None.

Example

To display dangerous messages on the master:

```
DWS-3160-24PC:admin# show attack_log index 1
Command: show attack_log index 1

Index   Date       Time      Level     Log Text
----- ---------- -------- -------- -------------------------------------------
1      2008-10-17 15:00:14 CRIT(2)   Land attack is blocked from (IP:
10.72.24.1  Port: 7)

DWS-3160-24PC:admin#
```

69-14 clear attack_log

Description

This command is used to clear the attack log.

Format

clear attack_log

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the master's attack log:

```
DWS-3160-24PC:admin# clear attack_log
Command: clear attack_log

Success.

DWS-3160-24PC:admin#
```

Chapter 70 System Severity Command List

config system_severity [trap | log | all] [emergency | alert| critical | error | warning | notice | information | debug | <level 0-7>]

show system_severity

70-1 config system_severity

Description

This command is used to configure the severity level control for the system. When the user chooses a specific level to log or trap, messages at that severity level or more will be logged or trapped to SNMP managers.

Format

config system_severity [trap | log | all] [emergency | alert| critical | error | warning | notice | information | debug | <level 0-7>]

Parameters

trap - Specifies the severity level control for traps.

log - Specifies the severity level control for the log.

all - Specifies the severity level control for traps and the log.

emergency - Severity level 0.
alert - Severity level 1.
critical - Severity level 2.
error - Severity level 3.
warning - Severity level 4.
notice - Severity level 5.
information - Severity level 6.
debug - Severity level 7.
<level 0-7> - Enter the severity level here. This value must be between 0 and 7.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure severity level control as information level for trap:

```
DWS-3160-24PC:admin# config system_severity trap information
Command: config system_severity trap information

Success.

DWS-3160-24PC:admin#
```

70-2 show system_severity

Description

This command is used to display the severity level controls for the system.

Format

show system_severity

Parameters

None.

Restrictions

None.

Example

To display severity level control for system:

```
DWS-3160-24PC:admin#show system_severity
Command: show system_severity

System Severity Trap : information(6)
System Severity Log : information(6)

DWS-3160-24PC:admin#
```

Chapter 71 TELNET Client Command List

telnet [<ipaddr> | <ipv6addr>] {tcp_port <value 1-65535>}

71-1 telnet

Description

This command is used to start the TELNET client to connect to the specific TELNET server. The parameters specified by the command will only be used for the establishment of this specific session. They will not affect the establishment of other sessions.

Format

telnet [<ipaddr> | <ipv6addr>] {tcp_port <value 1-65535>}

Parameters

<ipaddr> - The IP address of the TELNET server.
<ipv6addr> - The IPv6 address of the TELNET server.

tcp_port - (Optional) Specifies the TELNET server port number to be connected. If not specified, the default port is 23.
<value 1-65535> - Enter the TCP port number used here. This value must be between 1 and 65535.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

TELNET to a Switch by Specifiesing the IP address:

```
DWS-3160-24PC:admin# telnet 10.90.90.90
Command: telnet 10.90.90.90

                     DWS-3160-24TC Gigabit Ethernet Switch
                             Command Line Interface

                            Firmware: Build 1.00.034
           Copyright(C) 2012 D-Link Corporation. All rights reserved.

UserName:
```

Chapter 72 TFTP Client Command List

download [firmware_fromTFTP [<ipaddr> | <ipv6addr>] src_file <path_filename 64> {dest_file <pathname 64>} | cfg_fromTFTP [<ipaddr> | <ipv6addr>] src_file <path_filename 64> {dest_file <pathname 64>}]

upload [cfg_toTFTP [<ipaddr> | <ipv6addr>] dest_file <path_filename 64> {src_file <pathname 64>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}} | log_toTFTP [<ipaddr> | <ipv6addr>] dest_file <path_filename 64> | attack_log_toTFTP [<ipaddr> | <ipv6addr>] dest_file <path_filename 64> | firmware_toTFTP [<ipaddr> | <ipv6addr>] dest_file <path_filename 64> {src_file <path_filename 64>}]

72-1 download

Description

This command is used to download the firmware image and configuration from TFTP server.

Format

download [firmware_fromTFTP [<ipaddr> | <ipv6addr>] src_file <path_filename 64> {dest_file <pathname 64>} | cfg_fromTFTP [<ipaddr> | <ipv6addr>] src_file <path_filename 64> {dest_file <pathname 64>}]

Parameters

firmware_fromTFTP – Specifies to download firmware from a TFTP server.

<ipaddr> - (Optional) The IP address of the TFTP server.
<ipv6addr> - (Optional) The IPv6 address of the TFTP server.

src_file - (Optional) Used to identify the parameter “path_filename”.
<path_filename 64> - Enter the source file path name here. This name can be up to 64 characters long.

dest_file - (Optional) Used to identify the parameter “path_filename”.
<pathname 64> - Enter the destination file path name here. This name can be up to 64 characters long.

cfg_fromTFTP – Specifies to download a configuration file from a TFTP server.

<ipaddr> - (Optional) The IP address of the TFTP server.
<ipv6addr> - (Optional) The IPv6 address of the TFTP server.

src_file - (Optional) Used to identify the parameter “path_filename”.
<path_filename 64> - The pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

dest_file - (Optional) Used to identify the parameter “path_filename”.
<pathname 64> - The pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot_up configuration file. This name can be up to 64 characters long.

Restrictions

Only Administrators can issue this command.

Example

To download firmware from TFTP:

```
DWS-3160-24PC:admin# download firmware_fromTFTP 10.54.71.1 src_file px.had
Command: download firmware_fromTFTP 10.54.71.1 src_file px.had

Connecting to server................... Done.
Download firmware...................... Done.  Do not power off!
Please wait, programming flash......... Done.

DWS-3160-24PC:admin#
```

To download configuration from TFTP:

```
DWS-3160-24PC:admin# download cfg_fromTFTP 10.54.71.1 src_file cfg01.txt
Command: download cfg_fromTFTP 10.54.71.1 src_file cfg01.txt

Connecting to server................... Done.
Download configuration................. Done.

DWS-3160-24PC:admin#
```

72-2 upload

Description

This command is used to upload firmware and configuration from device to TFTP server.

Format

upload [cfg_toTFTP [<ipaddr> | <ipv6addr>] dest_file <path_filename 64> {src_file <pathname 64>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}} | log_toTFTP [<ipaddr> | <ipv6addr>] dest_file <path_filename 64> | attack_log_toTFTP [<ipaddr> | <ipv6addr>] dest_file <path_filename 64> | firmware_toTFTP [<ipaddr> | <ipv6addr>] dest_file <path_filename 64> {src_file <path_filename 64>}]

Parameters

cfg_toTFTP – Specifies that the configuration file will be uploaded to the TFTP server.
<ipaddr> - (Optional) The IP address of the TFTP server. **<ipv6addr>** - (Optional) The IPv6 address of the TFTP server.
dest_file - (Optional) Used to identify the parameter “path_filename”. **<path_filename 64>** - The pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.
src_file - (Optional) Used to identify the parameter “path_filename”. **<pathname 64>** - The pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot_up CFG file. This name can be up to 64 characters long.
<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

include - (Optional) Specifies to include lines that contain the specified filter string.
exclude - (Optional) Specifies to exclude lines that contain the specified filter string.
begin - (Optional) The first line that contains the specified filter string will be the first line of the output.

log_toTFTP – Specifies that the log file will be uploaded to the TFTP server.

<ipaddr> - (Optional) The IP address of the TFTP server.
<ipv6addr> - (Optional) The IPv6 address of the TFTP server.

dest_file - (Optional) Used to identify the parameter “path_filename”.
<path_filename 64> - The pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

attack_log_toTFTP – Specifies that the attack log will be uploaded to the TFTP server.

<ipaddr> - (Optional) The IP address of the TFTP server.
<ipv6addr> - (Optional) The IPv6 address of the TFTP server.

dest_file - (Optional) Used to identify the parameter “path_filename”.
<path_filename 64> - Specifies the path name on the TFTP server to hold the attack log. This name can be up to 64 characters long.

firmware_toTFTP – Specifies that the firmware file will be uploaded to the TFTP server.

<ipaddr> - (Optional) The IP address of the TFTP server.
<ipv6addr> - (Optional) The IPv6 address of the TFTP server.

dest_file - (Optional) Used to identify the parameter “path_filename”.
<path_filename 64> - The pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

src_file - (Optional) Used to identify the parameter “path_filename”.
<path_filename 64> - The pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot_up image. This name can be up to 64 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To upload firmware from a file system device to a TFTP server:

```
DWS-3160-24PC:admin# upload firmware_toTFTP 10.1.1.1 dest_file D:\firmware.had
src_file 100b70.had
Command: upload firmware_toTFTP 10.1.1.1 dest_file D:\firmware.had src_file
100b70.had

Connecting to server................... Done.
Upload firmware........................ Done.

DWS-3160-24PC:admin#
```

In case that the designated file does not exist:

```
DWS-3160-24PC:admin# upload firmware_toTFTP 10.1.1.1 dest_file D:\firmware.had
src_file 100b70.had
Command: upload firmware_toTFTP 10.1.1.1 dest_file D:\firmware.had src_file
100b70.had


 No such file.


 Failure!


DWS-3160-24PC:admin#
```

To upload configuration from TFTP:

```
DWS-3160-24PC:admin#upload cfg_toTFTP 10.90.90.99 dest_file 111.cfg src_file
c:/config.cfg
Command: upload cfg_toTFTP 10.90.90.99 dest_file 111.cfg src_file c:/config.cfg


 Connecting to server................... Done.
 Upload configuration................... Done.


DWS-3160-24PC:admin#
```

In case that the designated file does not exist:

```
DWS-3160-24PC:admin#upload cfg_toTFTP 10.90.90.99 dest_file 111.cfg src_file
c:/config2.cfg
Command: upload cfg_toTFTP 10.90.90.99 dest_file 111.cfg src_file
c:/config2.cfg


 No such file.


 Failure!


DWS-3160-24PC:admin#
```

To upload the master’s dangerous log:

```
DWS-3160-24PC:admin# upload attack_log_toTFTP 10.90.90.1 dest_file c:\alert.txt
Command: upload attack_log_toTFTP 10.90.90.1 dest_file c:\alert.txt


Success.


DWS-3160-24PC:admin#
```

Chapter 73 Time and SNTP Command List

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}
show sntp
enable sntp
disable sntp
config time <date ddmthyyyy> <time hh:mm:ss>
config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}
config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]
show time

73-1 config sntp

Description

This command is used to configure the Simple Network Time Protocol (SNTP) feature.

Format

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}

Parameters

primary - (Optional) SNTP primary server IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
secondary - (Optional) SNTP secondary server IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
poll-interval - (Optional) Specifies the polling interval range seconds. **<int 30-99999>** - Enter the polling interval range here. This value must be between 30 and 99999 seconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure SNTP:

```
DWS-3160-24PC:admin# config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-
interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

DWS-3160-24PC:admin#
```

73-2 show sntp

Description

This command is used to display the SNTP current time source and configuration.

Format

show sntp

Parameters

None.

Restrictions

None.

Example

To display SNTP:

```
DWS-3160-24PC:admin#show sntp
Command: show sntp

     Current Time Source   : System Clock
     SNTP                  : Disabled
     SNTP Primary Server   : 10.1.1.1
     SNTP Secondary Server : 10.1.1.2
     SNTP Poll Interval    : 30 sec

DWS-3160-24PC:admin#
```

73-3 enable sntp

Description

This command is used to enable the SNMP feature.

Format

enable sntp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable SNTP:

```
DWS-3160-24PC:admin# enable sntp
Command: enable sntp

Success.

DWS-3160-24PC:admin#
```

73-4 disable sntp

Description

This command is used to disable the SNTP feature.

Format

disable sntp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable SNTP:

```
DWS-3160-24PC:admin# disable sntp
Command: disable sntp

Success.

DWS-3160-24PC:admin#
```

73-5 config time

Description

This command is used to configure the time and date settings of the Switch.

Format

config time <date ddmthyyyy> <time hh:mm:ss>

Parameters

<date ddmthyyyy> - Specifies the system clock date. An example would look like this: '19sep2011'.

<time hh:mm:ss> - Specifies the system clock time. An example would look like this: '12:00:00'.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the time and date:

```
DWS-3160-24PC:admin#config time 19sep2011 16:30:30
Command: config time 19sep2011 16:30:30

Success.

DWS-3160-24PC:admin#
```

73-6 config time_zone

Description

This command is used to configure time zone of the Switch.

Format

config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}

Parameters

operator - (Optional) Specifies the operator of time zone.
    [+ | -] - Specifies that time should be added or subtracted to or from the GMT.

hour - (Optional) Specifies the hour of time zone.
    <gmt_hour 0-13> - Enter the hour value of the time zone here. This value must be between 0 and 13.

min - (Optional) Specifies the minute of time zone.
    <minute 0-59> - Enter the minute value of the time zone here. This value must be between 0 and 59.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure time zone:

```
DWS-3160-24PC:admin#config time_zone operator + hour 8 min 00
Command: config time_zone operator + hour 8 min 0

Success.

DWS-3160-24PC:admin#
```

73-7 config dst

Description

This command is used to configure the Daylight Saving Time (DST) of the Switch.

Format

config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]

Parameters

disable - Disable the Daylight Saving Time of the Switch.

repeating - Set the Daylight Saving Time to repeating mode.

- **s_week, e_week** - (Optional) Configure the start /end week number of Daylight Saving Time.
  - **<start_week 1-4, last>** - Enter the starting week number of Daylight Saving Time here. This value must be between 1 and 4.
  - **<end_week 1-4, last>** - Enter the ending week number of Daylight Saving Time here. This value must be between 1 and 4.
- **s_day, e_day** - (Optional) Configure the start /end day number of Daylight Saving Time.
  - **<start_day sun-sat>** - Enter the starting day value of Daylight Saving Time here. This value must either be sun, mon, tue, wed, thu, fri or sat.
  - **<end_day sun-sat>** - Enter the ending day value of Daylight Saving Time here. This value must either be sun, mon, tue, wed, thu, fri or sat.
- **s_mth, e_mth** - (Optional) Configure the start /end month number of Daylight Saving Time.
  - **<start_mth 1-12>** - Enter the starting month number of Daylight Saving Time here. This value must be between 1 and 12.
  - **<end_mth 1-12>** - Enter the ending month number of Daylight Saving Time here. This value must be between 1 and 12.
- **s_time, e_time** - (Optional) Configure the start /end time of Daylight Saving Time.
  - **<start_time hh:mm>** - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.
  - **<end_time hh:mm>** - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.
- **offset** - (Optional) Indicates number of minutes to add or to subtract during summertime. The ranges of offset are 30, 60, 90, and 120. The default value is 60.
  - **30** - Specifies that the offset range will 30 minutes.
  - **60** - Specifies that the offset range will 60 minutes.
  - **90** - Specifies that the offset range will 90 minutes.
  - **120** - Specifies that the offset range will 120 minutes.

annual - Set the Daylight Saving Time to annual mode.

s_date, e_date - (Optional) Configure the start /end date of Daylight Saving Time.

<start_date 1-31> - Enter the starting date of Daylight Saving Time here. This range must be between 1 an 31.

<end_date 1-31> - Enter the ending date of Daylight Saving Time here. This range must be between 1 an 31.

s_mth, e_mth - (Optional) Configure the start /end month number of Daylight Saving Time.

<start_mth 1-12> - Enter the starting month number of Daylight Saving Time here. This value must be between 1 and 12.

<end_mth 1-12> - Enter the ending month number of Daylight Saving Time here. This value must be between 1 and 12.

s_time, e_time - (Optional) Configure the start /end time of Daylight Saving Time.

<start_time hh:mm> - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.

<end_time hh:mm> - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.

offset - (Optional) Indicates number of minutes to add or to subtract during summertime. The ranges of offset are 30, 60, 90,120; default value is 60.

30 - Specifies that the offset range will 30 minutes.

60 - Specifies that the offset range will 60 minutes.

90 - Specifies that the offset range will 90 minutes.

120 - Specifies that the offset range will 120 minutes.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure DST:

```
DWS-3160-24PC:admin#config dst repeating s_week 2 s_day tue s_mth 4 s_time
15:00 e_week 2 e_day wed e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2
e_day wed e_mth 10 e_time 15:30 offset 30


Success.


DWS-3160-24PC:admin#
```

73-8 show time

Description

This command is used to display the time states.

Format

show time

Parameters

None.

Restrictions

None.

Example

To display the time:

```
DWS-3160-24PC:admin#show time
Command: show time

     Current Time Source  : System Clock
     Boot Time    : 19 Sep 2011  23:50:43
     Current Time : 20 Sep 2011  01:01:51
     Time Zone    : GMT +08:00
     Daylight Saving Time  : Repeating
         Offset In Minutes : 30
         Repeating    From : Apr 2nd  Tue 15:00
                      To   : Oct 2nd  Wed 15:30
         Annual       From : 29 Apr 00:00
                      To   : 12 Oct 00:00

DWS-3160-24PC:admin#
```

Chapter 74 Trace Route Command List

traceroute <ipaddr> {ttl <value 1-60>} {port <value 30000-64900>} {timeout <sec 1-65535>} {probe <value 1-9>}
traceroute6 <ipv6addr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

74-1 traceroute

Description

This command is used to trace a routed path between the Switch and a destination end station.

Format

traceroute <ipaddr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

Parameters

<ipaddr> - Specifies the IP address of the destination end station.
ttl - (Optional) The time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass. The traceroute command will cross while seeking the network path between two devices. The range for the TTL is 1 to 60 hops. **<value 1-60>** - Enter the time to live value here. This value must be between 1 and 60.
port - (Optional) The port number. The value range is from 30000 to 64900. **<value 30000-64900>** - Enter the port number here. This value must be between 30000 and 64900.
timeout - (Optional) Defines the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds. **<sec 1-65535>** - Enter the timeout period value here. This value must be between 1 and 65535 seconds.
probe - (Optional) The number of probing. The range is from 1 to 9. If unspecified, the default value is 1. **<value 1-9>** - Enter the probing number value here. This value must be between 1 and 9.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To trace the routed path between the Switch and 10.48.74.121:

```
DWS-3160-24PC:admin#traceroute 72.14.203.106
Command: traceroute 72.14.203.106

 <10 ms  10.1.1.254
 <10 ms  192.168.249.129
 <10 ms  192.168.15.254
 <10 ms  192.168.5.230
 20  ms  124.219.29.126
 20  ms  203.207.46.125
 30  ms  203.207.47.49
 20  ms  203.79.222.137
 20  ms  211.76.96.61
 20  ms  72.14.196.13
 20  ms  209.85.243.26
 20  ms  209.85.250.101
 20  ms  209.85.241.162
 20  ms  72.14.203.106

Trace complete.

DWS-3160-24PC:admin#
```

74-2 traceroute6

Description

This command is used to trace the IPv6 routed path between the Switch and a destination end station.

Format

traceroute6 <ipv6addr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

Parameters

<ipv6addr> - Specifies the IPv6 address of the destination end station.

ttl - (Optional) The time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass. The traceroute command will cross while seeking the network path between two devices. The range for the TTL is 1 to 60 hops.
<value 1-60> - Enter the time to live value here. This value must be between 1 and 60.

port - (Optional) The port number. The value range is from 30000 to 64900.
<value 30000-64900> - Enter the port number here. This value must be between 30000 and 64900.

timeout - (Optional) Defines the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.
<sec 1-65535> - Enter the timeout period value here. This value must be between 1 and 65535 seconds.

probe - (Optional) The number of probing. The range is from 1 to 9. If unspecified, the default value is 1.
<value 1-9> - Enter the probing number value here. This value must be between 1 and 9.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To trace the IPv6 routed path between the Switch and 3000::1:

```
DWS-3160-24PC:admin# traceroute6 3000::1 probe 3
Command: traceroute6 3000::1 probe 3

1   <10 ms.     1345:142::11
2   <10 ms.     2011:14::100
3   <10 ms.     3000::1

Trace complete.

DWS-3160-24PC:admin#
```

To trace the IPv6 routed path between the Switch and 1210:100::11 with port 40000:

```
DWS-3160-24PC:admin# traceroute6 1210:100::11 port 40000
Command: traceroute6 1210:100::11 port 40000

1   <10 ms.     3100::25
2   <10 ms.     4130::100
3   <10 ms.     1210:100::11

Trace complete.

DWS-3160-24PC:admin#
```

Chapter 75 Traffic Control Command List

config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] |unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | countdown [<min 0> | <min 3-30> | disable] | time_interval <sec 5-600>}
config traffic trap [none | storm_occurred | storm_cleared | both]
show traffic control {<portlist>}
config traffic control log state [enable | disable]
config traffic control auto_recover_time [<min 0> | <min 1-65535>]

75-1 config traffic control

Description

This command is used to configure broadcast/ multicast/ unicast packet storm control. Shutdown mode is provided to monitor the traffic rate in addition to the storm control drop mode. If traffic rate is too high, this port will be shut down.

Format

config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | countdown [<min 0> | <min 3-30> | disable] | time_interval <sec 5-600>}

Parameters

<portlist> - Used to Specifies a range of ports to be configured. **all** - Specifies that all the ports will be used for this configuration.
broadcast - (Optional) Enable or disable broadcast storm control. **enable** - Specifies that broadcast storm control will be enabled. **disable** - Specifies that broadcast storm control will be disabled.
multicast - (Optional) Enable or disable multicast storm control. **enable** - Specifies that multicast storm control will be enabled. **disable** - Specifies that multicast storm control will be disabled.
unicast - (Optional) Enable or disable unknown packet storm control. (Supported for drop mode only) **enable** - Specifies that unicast storm control will be enabled. **disable** - Specifies that unicast storm control will be disabled.
action - (Optional) One of the two options for action is specified for storm control, shutdown or drop mode. Shutdown mode is a function of software, drop mode is implemented by the chip. If shutdown mode is specified, it is necessary to configure values for the countdown and time_interval parameters. **drop** - Specifies that the action applied will be drop mode. **shutdown** - Specifies that the action applied will be shutdown mode.
threshold - (Optional) The upper threshold, at which point the specified storm control is triggered. The <value> is the number of broadcast/multicast packets per second received by the Switch that will trigger the storm traffic control measure. The threshold is expressed as PPS (packets per second) and must be an unsigned integer. **<value 0-255000>** - Enter the upper threshold value here. This value must be between 0 and 255000.
countdown - (Optional) Timer for shutdown mode. If a port enters the shutdown Rx state and

this timer runs out, port will be shutdown forever. The parameter is not applicable if “drop” (mode) is specified for the “action” parameter.
<min 0> - 0 disables the forever state, meaning that the port will not enter the shutdown forever state.
<min 3-30> - Enter the countdown timer value here. This value must be between 3 and 30.
disable – Specifies that the countdown timer will be disabled.

time_interval - (Optional) The sampling interval of received packet counts. The possible value will be m-n seconds. The parameter is not applicable if “drop” (mode) is specified for the “action” parameter.
<sec 5-600> - Enter the time interval value here. This value must be between 5 and 600.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the parameters so that the traffic control status is enabled on ports 1-12:

```
DWS-3160-24PC:admin# config traffic control 1-12 broadcast enable action
shutdown threshold 1 countdown 5 time_interval 10
Command: config traffic control 1-12 broadcast enable action shutdown threshold
1 countdown 5 time_interval 10


Success.


DWS-3160-24PC:admin#
```

75-2 config traffic trap

Description

This command is used to configure trap modes.

Occurred Mode: This trap is sent when a packet storm is detected by the packet storm mechanism.

Cleared Mode: This trap is sent when the packet storm is cleared by the packet storm mechanism.

Format

config traffic trap [none | storm_occurred | storm_cleared | both]

Parameters

none - No trap state is specified for storm control.

storm_occurred - Occurred mode is enabled and cleared mode is disabled.

storm_cleared - Occurred mode is disabled and cleared mode is enabled.

both - Both occurred and cleared modes are enabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable both the occurred mode and cleared mode traffic control traps:

```
DWS-3160-24PC:admin# config traffic trap both
Command: config traffic trap both

Success.

DWS-3160-24PC:admin#
```

75-3 show traffic control

Description

This command is used to display the current traffic control settings.

Format

show traffic control {<portlist>}

Parameters

<portlist> - (Optional) Used to Specifies the range of ports to be displayed.

If no parameter is specified, the system will display the packet storm control configuration for all ports.

Restrictions

None.

Example

To display the traffic control parameters for ports 1 to 10:

```
DWS-3160-24PC:admin#show traffic control 1-10
Command: show traffic control 1-10

Traffic Control Trap             : [Both]
Traffic Control Log              : Enabled
Traffic Control Auto Recover Time: 0 Minutes

Port Thres  Broadcast Multicast Unicast  Action   Count    Time     Shutdown
     hold   Storm     Storm     Storm             down     Interval Forever
---- ------ --------- --------- -------- -------- -------- -------- --------
1    1      Enabled   Disabled  Disabled shutdown 5        10
2    1      Enabled   Disabled  Disabled shutdown 5        10
3    1      Enabled   Disabled  Disabled shutdown 5        10
4    1      Enabled   Disabled  Disabled shutdown 5        10
5    1      Enabled   Disabled  Disabled shutdown 5        10
6    1      Enabled   Disabled  Disabled shutdown 5        10
7    1      Enabled   Disabled  Disabled shutdown 5        10
8    1      Enabled   Disabled  Disabled shutdown 5        10
9    1      Enabled   Disabled  Disabled shutdown 5        10
10   1      Enabled   Disabled  Disabled shutdown 5        10

DWS-3160-24PC:admin#
```

75-4 config traffic control log state

Description

This command is used to configure the traffic control log state. When the log state is enabled, traffic control states are logged when a storm occurs and when a storm is cleared. If the log state is disabled, traffic control events are not logged.

NOTE: The log state is only applicable for shutdown mode. Since shutdown mode only support broadcast and multicast storm control, doesn’t support unicast storm control. The log only generate for broadcast and multicast storm control.

Format

config traffic control log state [enable | disable]

Parameters

enable - Both occurred and cleared are logged.
disable - Neither occurred nor cleared is logged.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the traffic log state on the Switch:

```
DWS-3160-24PC:admin# config traffic control log state enable
Command: config traffic control log state enable

Success.

DWS-3160-24PC:admin#
```

75-5 config traffic control auto_recover_time

Description

This command is used to configure the traffic auto recover time that allowed for a port to recover from shutdown forever status.

Format

config traffic control auto_recover_time [<min 0> | <min 1-65535>]

Parameters

auto_recover_time - The time allowed for auto recovery from shutdown for a port. The default value is 0, so no auto recovery is possible; the port remains in shutdown forever mode. This requires manual entry of the CLI command “config ports [<portlist> | all] state enable" to return the port to a forwarding state. The default value is 0, which means disable auto recover mode, shutdown forever.

<min 0> - Specifies that the auto recovery time will be disabled.

<min 1-65535> - Enter the auto recovery time value here. This value must be between 1 and 65535.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the auto recover time to 5 minutes:

```
DWS-3160-24PC:admin# config traffic control auto_recover_time 5
Command: config traffic control auto_recover_time 5

Success.

DWS-3160-24PC:admin#
```

Chapter 76 Traffic Segmentation Command List

config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]
show traffic_segmentation {<portlist>}

76-1 config traffic_segmentation

Description

This command is used to configure the traffic segmentation.

Format

config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]

Parameters

<portlist> - Specifies a range of ports to be configured. **all -** Specifies that all the ports will be used for this configuration.
forward_list - Specifies a range of port forwarding domain. **null** - Specifies a range of port forwarding domain is null. **all** – Specifies all ports to be configured. **<portlist>** - Specifies a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure traffic segmentation:

```
DWS-3160-24PC:admin# config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15

Success.

DWS-3160-24PC:admin#
```

76-2 show traffic_segmentation

Description

This command is used to display current traffic segmentation table.

Format

show traffic_segmentation {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be displayed.

If no parameter is specified, the system will display all current traffic segmentation tables.

Restrictions

None.

Example

To display traffic segmentation table:

```
DWS-3160-24PC:admin#show traffic_segmentation 1-10
Command: show traffic_segmentation 1-10

Traffic Segmentation Table

Port  Forward Portlist
----  ------------------------------------------------------------------------
1      11-15
2      11-15
3      11-15
4      11-15
5      11-15
6      11-15
7      11-15
8      11-15
9      11-15
10     11-15

DWS-3160-24PC:admin#
```

Chapter 77 Trusted Host Command List

create trusted_host [<ipaddr> |<ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] {snmp | telnet | ssh | http | https | ping}
delete trusted_host [ipaddr <ipaddr> | ipv6address <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr> | all]
config trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] [add | delete] {snmp | telnet | ssh | http | https | ping | all}
show trusted_host

77-1 create trusted_host

Description

This command is used to create the trusted host. The Switch allows you to Specifies up to three IP addresses that are allowed to manage the Switch via in-band SNMP or TELNET 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.

When the access interface is not specified, the trusted host will be created for all interfaces.

Format

create trusted_host [<ipaddr> |<ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] {snmp | telnet | ssh | http | https | ping}

Parameters

<ipaddr> - Enter the IP address of the trusted host here. **<ipv6addr>** - Enter the IPv6 address of the trusted host here.
network – Specifies the network address of the trusted network. **<network_address>** - Enter the network address used here.
ipv6_prefix – Specifies that IPv6 prefix here. **<ipv6networkaddr>** - Enter the IPv6 network address here.
snmp - (Optional) Specifies trusted host for SNMP. **telnet** - (Optional) Specifies trusted host for TELENT. **ssh** - (Optional) Specifies trusted host for SSH **http** - (Optional) Specifies trusted host for HTTP **https** - (Optional) Specifies trusted host for HTTPs. **ping** - (Optional) Specifies trusted host for PING

Restrictions

Only Administrators and Operators can issue this command.

Example

To create the trusted host:

```
DWS-3160-24PC:admin# create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DWS-3160-24PC:admin#
```

77-2 delete trusted_host

Description

This command is used to delete a trusted host entry from the database.

Format

delete trusted_host [ipaddr <ipaddr> | ipv6address <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr> | all]

Parameters

ipaddr - The IP address of the trusted host.
    <ipaddr> - Enter the IP address used for this configuration here.

ipv6addr - The IPv6 address of the trusted host.
    <ipv6addr> - Enter the IPv6 address used for this configuration here.

network - The network address of the trusted network.
    <network_address> - Enter the network address used for this configuration here.

ipv6_prefix - The IPv6 subnet prefix of the trusted network.
    <ipv6networkaddr> - Enter the IPv6 subnet prefix here.

all - All trusted hosts will be deleted.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the trusted host:

```
DWS-3160-24PC:admin# delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.

DWS-3160-24PC:admin#
```

77-3 config trusted_host

Description

This command is used to configure the access interfaces for the trusted host.

Format

config trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] [add | delete] {snmp | telnet | ssh | http | https | ping | all}

Parameters

<ipaddr> - Enter the IP address of the trusted host here.
<ipv6addr> - Enter the IPv6 address of the trusted host here.

network – Specifies the network address of the trusted network.
  <network_address> - Enter the network address used here.

ipv6_prefix – Specifies the IPv6 subnet prefix of the trusted network.
  <ipv6networkaddr> - Enter the IPv6 subnet prefix here.

add - Add interfaces for that trusted host.
delete - Delete interfaces for that trusted host.

snmp - (Optional) Specifies trusted host for SNMP.
telnet - (Optional) Specifies trusted host for TELENT.
ssh - (Optional) Specifies trusted host for SSH.
http - (Optional) Specifies trusted host for HTTP.
https - (Optional) Specifies trusted host for HTTPs.
ping - (Optional) Specifies trusted host for PING.
all – (Optional) Specifies trusted host for all application.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the trusted host:

```
DWS-3160-24PC:admin# config trusted_host 10.48.74.121 add ssh telnet
Command: config trusted_host 10.48.74.121 add ssh telnet

Success.

DWS-3160-24PC:admin#
```

77-4 show trusted_host

Description

This command is used to display a list of trusted hosts on the Switch.

Format

show trusted_host

Parameters

None.

Restrictions

None.

Example

To display trusted hosts:

```
DWS-3160-24PC:admin#show trusted_host
Command: show trusted_host

Management Stations

IP Address                                  Access Interface
----------------------------------------------------------------
10.48.74.121/32                             SNMP Telnet SSH HTTP HTTPs Ping
1234::1                                     SNMP HTTP
1234::                                      SNMP Telnet HTTP

Total Entries: 3

DWS-3160-24PC:admin#
```

Chapter 78 Unicast Routing Command List

create iproute [default] <ipaddr> {<metric 1-65535>} {[primary | backup]}
delete iproute [default | <network_address>] <ipaddr>
show iproute {static}
show ipfdb {[ip_address <ipaddr> | interface <ipif_name 12> | port <port>]}

78-1 create iproute

Description

This command is used to create a static IP route. Selecting “primary” or “backup” means the newly created route is a floating static route. If none of the following, “primary” or “backup”, is selected, the default route will:

1. Be primary if there is no primary route that has the same destination;
2. Be backup if there has been a primary route that has the same destination.
3. Fail to create if there have been a primary route and a backup route that have the same destination.
4. Fail to create if there has been one static multipath route that has the same destination.

It will fail if a user wants to create a floating static route and there has been one static multipath route with the same destination.

It will fail if a user wants to create a static multipath route and there has been a floating static route, whether primary or backup.

Format

create iproute [default] <ipaddr> {<metric 1-65535>} {[primary | backup]}

Parameters

default - Create an IP default route (0.0.0.0/0).
<ipaddr> - The IP address for the next hop router.
<metric 1-65535> - (Optional) Enter the metric value here. This value must be between 1 and 65535. The default setting is 1.
primary - (Optional) Specifies the route as the primary route to the destination. **backup** - (Optional) Specifies the route as the backup route to the destination.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a floating static route and a static multipath route:

```
DWS-3160-24PC:admin# create iproute default 10.1.1.254 primary
Command: create iproute default 10.1.1.254 primary

Success.

DWS-3160-24PC:admin#
```

78-2 delete iproute

Description

This command is used to delete an IP route entry from the Switch's IP routing table.

Format

delete iproute [default | <network_address>] <ipaddr>

Parameters

default - Deletes an IP default route (0.0.0.0/0).
<network_address> – Specifies the network address used.

<ipaddr> - Specifies the next hop IP address of the route need to be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an IP default route:

```
DWS-3160-24PC:admin# delete iproute default 10.1.1.254
Command: delete iproute default 10.1.1.254

Success.

DWS-3160-24PC:admin#
```

78-3 show iproute

Description

This command is used to display the Switch's current IP routing table.

Format

show iproute {static}

Parameters

static – (Optional) Specifies that this route will be static.

Restrictions

None.

Example

To display the contents of the IP routing table:

```
DWS-3160-24PC:admin#show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway          Interface     Cost      Protocol
------------------  ---------------  ------------  --------  --------
0.0.0.0/0           192.168.69.1     System        1         Default
192.168.69.0/24     0.0.0.0          System        1         Local

Total Entries: 2

DWS-3160-24PC:admin#
```

78-4 show ipfdb

Description

This command is used to display the current network address forwarding database.

Format

show ipfdb {[ip_address <ipaddr> | interface <ipif_name 12> | port <port>]}

Parameters

ip_address - (Optional) Displays the specified host IP address. **<ipaddr>** - Enter the IP address used here.
interface - (Optional) Specifies a IP interface. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
port - (Optional) Specifies a port. **<port>** - Enter the port number here.

Restrictions

None.

Example

To display network address forwarding table:

```
DWS-3160-24PC:admin#show ipfdb
Command: show ipfdb

Interface     IP Address       Port    Learned
------------  ---------------  ------  ---------
System        192.168.69.1     1       Dynamic
System        192.168.69.66    1       Dynamic

Total Entries: 2

DWS-3160-24PC:admin#
```

Chapter 79 Virtual Router Redundancy Protocol (VRRP) Command List

enable vrrp {ping}

disable vrrp {ping}

create vrrp vrid <vrid 1-255> ipif <ipif_name 12> ipaddress <ipaddr> {state [enable | disable] | priority <int 1-254> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}

config vrrp vrid <vrid 1-255> ipif <ipif_name 12> {state [enable | disable] | priority <int 1-254> | ipaddress <ipaddr> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}

config vrrp ipif <ipif_name 12> [authtype [none | simple authdata <string 8> | ip authdata <string 16>]]

delete vrrp {vrid <vrid 1-255> ipif <ipif_name 12>}

show vrrp {ipif <ipif_name 12> {vrid <vrid 1-255>}}

79-1 enable vrrp

Description

This command is used to enable VRRP globally.

Format

enable vrrp {ping}

Parameters

ping - (Optional) Specifies that the ping option will be enabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable VRRP:

```
DWS-3160-24PC:admin# enable vrrp
Command: enable vrrp

Success.

DWS-3160-24PC:admin#
```

79-2 disable vrrp

Description

This command is used to disable VRRP globally.

Format

disable vrrp {ping}

Parameters

ping - (Optional) Specifies that the ping option will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable VRRP:

```
DWS-3160-24PC:admin# disable vrrp
Command: disable vrrp

Success.

DWS-3160-24PC:admin#
```

79-3 create vrrp vrid

Description

This command is used to create a virtual router entry by VRID.

Format

create vrrp vrid <vrid 1-255> ipif <ipif_name 12> ipaddress <ipaddr> {state [enable | disable] | priority <int 1-254> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}

Parameters

vrid - Specifies the ID of the Virtual Router used. **<vrid 1-255>** - Enter the Virtual Router ID used here. This value must be between 1 and 255.
ipif - Specifies the IP interface used for this configuration. **<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.
ipaddress - Specifies the virtual router’s IP address used. **<ipaddr>** - Enter the virtual router's IP address used here.
state - (Optional) Specifies the state of the virtual router function. **enable** - Specifies that the virtual router function will be enabled. **disable** - Specifies that the virtual router function will be disabled.

priority - (Optional) Specifies the priority to be used for the Virtual Router Master election process
<int 1-254> - Enter the priority value used here. This value must be between 1 and 254.

advertisement_interval - (Optional) Specifies the time interval used between sending advertisement messages.
<int 1-255> - Enter the advertisement interval value here. This value must be between 1 and 255 seconds.

preempt - (Optional) Controls whether a higher priority virtual router will preempt a lower priority master. The preempt setting must be consistent with all the routers participating within the same VRRP group. Default is settings is true.
true - Specifies that if the backup router's priority is set higher than the master's priority, it will become the master instead of the current one.
false - Specifies that if the backup router's priority is higher than the master's priority, it will not become the master until the master failed.

critical_ip - (Optional) Specifies an IP address that will provide the most direct route to the Internet or other critical network connections from this virtual router. This IP address must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, the virtual router will automatically be disabled. A new Master will be elected from the backup routers participating in the VRRP group. Different critical IP addresses may be assigned to different routers participating in the VRRP group and can therefore define multiple routes to the Internet or other critical network connections.
<ipaddr> - Enter the critical interface's IP address used here.

critical_ip_state - (Optional) Specifies the state of checking the status (active or inactive) of a critical IP address.
enable - Specifies that the critical IP state checking will be enabled.
disable - Specifies that the critical IP state checking will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a VRRP entry:

```
DWS-3160-24PC:admin# create vrrp vrid 1 ipif System ipaddress 10.90.90.91 state
enable
Command: create vrrp vrid 1 ipif System ipaddress 10.90.90.91 state enable

Success.

DWS-3160-24PC:admin#
```

79-4 config vrrp vrid

Description

This command is used to configure the virtual router settings by VRID.

Format

config vrrp vrid <vrid 1-255> ipif <ipif_name 12> {state [enable | disable] | priority <int 1-254> | ipaddress <ipaddr> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}

Parameters

vrid - specifies the ID of the Virtual Router used.
<vrid 1-255> - Enter the Virtual Router ID used here. This value must be between 1 and 255.

ipif - Specifies the IP interface used for this configuration.
<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

state - (Optional) Specifies the state of the virtual router function.
enable - Specifies that the virtual router function will be enabled.
disable - Specifies that the virtual router function will be disabled.

priority - (Optional) specifies the priority to be used for the Virtual Router Master election process
<int 1-254> - Enter the priority value used here. This value must be between 1 and 254.

ipaddress - (Optional) Specifies the virtual router's IP address used.
<ipaddr> - Enter the virtual router's IP address used here.

advertisement_interval - (Optional) Specifies the time interval used between sending advertisement messages.
<int 1-255> - Enter the advertisement interval value here. This value must be between 1 and 255 seconds.

preempt - (Optional) Controls whether a higher priority virtual router will preempt a lower priority master. The preempt setting must be consistent with all the routers participating within the same VRRP group. Default is setting is true.
true - Specifies that if the backup router's priority is set higher than the master's priority, it will become the master instead of the current one.
false - Specifies if the backup router's priority is higher than the master's priority, it will not become the master until the master failed.

critical_ip - (Optional) specifies an IP address that will provide the most direct route to the Internet or other critical network connections from this virtual router. This IP address must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, the virtual router will automatically be disabled. A new Master will be elected from the backup routers participating in the VRRP group. Different critical IP addresses may be assigned to different routers participating in the VRRP group and can therefore define multiple routes to the Internet or other critical network connections.
<ipaddr> - Enter the critical interface's IP address used here.

critical_ip_state - (Optional) Specifies the state of checking the status (active or inactive) of a critical IP address.
enable - Specifies that the critical IP state checking will be enabled.
disable - Specifies that the critical IP state checking will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure VRRP:

```
DWS-3160-24PC:admin# config vrrp vrid 1 ipif System state enable
Command: config vrrp vrid 1 ipif System state enable

Success.

DWS-3160-24PC:admin#
```

79-5 config vrrp ipif

Description

This command is used to configure a virtual router authentication type on an interface.

Format

config vrrp ipif <ipif_name 12> [authtype [none | simple authdata <string 8> | ip authdata <string 16>]]

Parameters

ipif - Specifies the name of IP interface used for this configuration.

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

authtype - Specifies the VRRP's authentication type.

none - Specifies that no authentication algorithm will be used on this interface.

simple - Specifies that the authentication algorithm will be set to simple text on this interface.

authdata - Specifies the authentication data used in the simple text authentication algorithm.

<string 8> - Enter the authentication data used in the simple text authentication algorithm here. This value can be up to 8 characters long.

ip - Specifies that the authentication algorithm will be set to IP authentication header on this interface.

authdata - Specifies the authentication data used in the IP authentication header algorithm.

<string 16> - Enter the authentication data used in the IP authentication header algorithm here. This value can be up to 16 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a VRRP IP interface:

```
DWS-3160-24PC:admin# config vrrp ipif System authtype simple authdata 12345678
Command: config vrrp ipif System authtype simple authdata 12345678

Success.

DWS-3160-24PC:admin#
```

79-6 delete vrrp

Description

This command is used to delete the VRRP entries.

Format

delete vrrp {vrid <vrid 1-255> ipif <ipif_name 12>}

Parameters

vrid - (Optional) Specifies the Virtual Router ID used.

<vrid 1-255> - Enter the Virtual Router ID used here. This value must be between 1 and 255.

ipif - (Optional) Specifies the IP interface name used.

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

If no parameter is specified, all the VRRP entries will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete VRRP:

```
DWS-3160-24PC:admin# delete vrrp vrid 3 ipif System
Command: delete vrrp vrid 3 ipif System

Success.

DWS-3160-24PC:admin#
```

79-7 show vrrp

Description

This command is used to display the VRRP settings.

Format

show vrrp {ipif <ipif_name 12> {vrid <vrid 1-255>}}

Parameters

ipif - (Optional) Specifies the IP interface name to be displayed.

<ipif_name 12> - Enter the IP interface name to be displayed here. This name can be up to 12 characters long.

vrid - (Optional) Specifies the Virtual Router ID to be displayed.

<vrid 1-255> - Enter the Virtual Router ID to be displayed here. This value must be between 1 and 255.

If no parameter is specified, then all the VRRP entries will be displayed.

Restrictions

None.

Example

To display the VRRP configuration:

```
DWS-3160-24PC:admin#show vrrp
Command: show vrrp

 Global VRRP            : Enabled
 Non-owner Response Ping: Disabled

 Interface Name                : System
 Authentication type           : Simple Text Password
 Authentication Data           : 12345678

         VRID                   : 1
         Virtual IP Address     : 10.90.90.91
         Virtual MAC Address    : 00-00-5E-00-01-01
         Virtual Router State   : Master
         State                  : Enabled
         Priority               : 100
         Master IP Address      : 10.90.90.90
         Critical IP Address    : 0.0.0.0
         Checking Critical IP   : Disabled
         Advertisement Interval : 1 secs
         Preempt Mode           : True
         Virtual Router Up Time : 10064 centi-secs

 Total Entries: 1

DWS-3160-24PC:admin#
```

Chapter 80 VLAN Trunking Command List

enable vlan_trunk

disable vlan_trunk

config vlan_trunk ports [<portlist> | all] | state [enable | disable]

show vlan_trunk

80-1 enable vlan_trunk

Description

This command is used to enable the VLAN trunk function. When the VLAN trunk function is enabled, the VLAN trunk ports shall be able to forward all tagged frames with any VID.

Format

enable vlan_trunk

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the VLAN Trunk:

```
DWS-3160-24PC:admin# enable vlan_trunk
Command: enable vlan_trunk

Success.

DWS-3160-24PC:admin#
```

80-2 disable vlan_trunk

Description

This command is used to disable the VLAN trunk function.

Format

disable vlan_trunk

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the VLAN Trunk:

```
DWS-3160-24PC:admin# disable vlan_trunk
Command: disable vlan_trunk

Success.

DWS-3160-24PC:admin#
```

80-3 config vlan_trunk

Description

This command is used to configure a port as a VLAN trunk port. By default, none of the port is a VLAN trunk port.

If the user enables the global VLAN trunk function and configure the VLAN trunk ports, then the trunk port will be member port of all VLANs. That is, if a VLAN is already configured by the user, but the trunk port is not member port of that VLAN, this trunk port will automatically become tagged member port of that VLAN. If a VLAN is not created yet, the VLAN will be automatically created, and the trunk port will become tagged member of this VLAN.

When the user disables the VLAN trunk globally, all VLANs automatically created by VLAN Trunk enabled shall be destroyed, and all the automatically added port membership will be removed.

A VLAN trunk port and a non-VLAN trunk port cannot be grouped as an aggregated link. To change the VLAN trunk setting for an aggregated link, the user must apply the command to the master port. However, this setting will disappear as the aggregated link is destroyed, and the VLAN trunk setting of the individual port will follow the original setting of the port.

If the command is applied to link aggregation member port excluding the master, the command will be rejected.

The ports with different VLAN configurations are not allowed to form an aggregated link. However, if they are specified as VLAN trunk port, they are allowed to form an aggregated link.

For a VLAN trunk port, the VLANs on which the packets can be by passed will not be advertised by GVRP on this port. However, since the traffic on these VLANs are forwarded, this VLAN trunk port should participate in the MSTP instances corresponding to these VLAN.

Format

config vlan_trunk ports [<portlist> | all] | state [enable | disable]

Parameters

<portlist> - Enter a list of ports used for the configuration here.
all - Specifies that all the ports will be used for this configuration.

state - Specifies that the port is a VLAN trunk port or not.
enable - Specifies that the port is a VLAN trunk port.
disable - Specifies that the port is not a VLAN trunk port.

Restrictions

Only Administrators can issue this command.

Example

To configure a VLAN trunk port:

```
DWS-3160-24PC:admin# config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

DWS-3160-24PC:admin#
```

Port 6 is LA-1 member port; port 7 is LA-2 master port:

```
DWS-3160-24PC:admin# config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

The link aggregation member port cannot be configured.
Fail.

DWS-3160-24PC:admin# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DWS-3160-24PC:admin# config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

The link aggregation member port cannot be configured.
Fail.

DWS-3160-24PC:admin#
```

Port 6 is LA-1 member port; port 7 is LA-1 master port:

```
DWS-3160-24PC:admin# config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Success.

DWS-3160-24PC:admin#
```

Port 6, 7 have different VLAN configurations before enabling VLAN trunk.

Port 6 is LA-1 member port; port 7 is LA-1 master port.

```
DWS-3160-24PC:admin# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

The link aggregation needs to be deleted first.
Fail.
```

Port 6, 7 have the same VLAN configuration before enabling VLAN trunk.

Port 6 is LA-1 member port; port 7 is LA-1 master port.

```
DWS-3160-24PC:admin# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DWS-3160-24PC:admin# config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Success.

DWS-3160-24PC:admin#
```

80-4 show vlan_trunk

Description

This command is used to display the VLAN trunk configuration.

Format

show vlan_trunk

Parameters

None.

Restrictions

None.

Example

To display the VLAN Trunk information:

```
DWS-3160-24PC:admin#show vlan_trunk
Command: show vlan_trunk

VLAN Trunk Global Setting
----------------------------
VLAN Trunk Status  : Enabled
VLAN Trunk Member Ports : 1-7

DWS-3160-24PC:admin#
```

The following example displays the VLAN information which will also display VLAN trunk setting:

```
DWS-3160-24PC:admin#show vlan
Command: show vlan

VLAN Trunk State        : Enabled
VLAN Trunk Member Ports : 1-7

VID             : 1               VLAN Name     : default
VLAN Type       : Static          Advertisement : Enabled
Member Ports    : 1-24
Static Ports    : 1-24
Current Tagged Ports  :
Current Untagged Ports: 1-24
Static Tagged Ports   :
Static Untagged Ports : 1-24
Forbidden Ports       :

Total Static VLAN Entries: 1
Total GVRP VLAN Entries: 0

DWS-3160-24PC:admin#
```

Chapter 81 Voice VLAN Command List

enable voice_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>]
disable voice_vlan
config voice_vlan priority <int 0-7>
config voice_vlan oui [add | delete] <macaddr> <macmask> {description <desc 32>}
config voice_vlan ports [<portlist> | all] [state [enable | disable] | mode [auto | manual]]
config voice_vlan aging_time <min 1-65535>
show voice_vlan
show voice_vlan oui
show voice_vlan ports {<portlist>}
show voice_vlan voice_device {ports <portlist>}
config voice_vlan log state [enable | disable]

81-1 enable voice_vlan

Description

This command is used to enable the global voice VLAN function on a Switch. To enable the voice VLAN, the voice VLAN must be also assigned .At the same time, the VLAN must be an existing static 802.1Q VLAN. To change the voice VLAN, the user must disable the voice VLAN function, and re-issue this command. By default, the global voice VLAN state is disabled.

Format

enable voice_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

<vlan_name 32> - Enter the name of the voice VLAN here. This name can be up to 32 characters long.

vlanid - Specifies the VLAN ID of the voice VLAN.

<vlanid 1-4094> - Enter the voice VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable a voice VLAN with name “v2”:

```
DWS-3160-24PC:admin# enable voice_vlan v2
Command: enable voice_vlan v2

Success.
DWS-3160-24PC:admin#
```

81-2 disable voice_vlan

Description

The command is used to disable the voice VLAN function on a Switch. When the voice VLAN function is disabled, the voice VLAN will become unassigned.

Format

disable voice_vlan

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the voice VLAN:

```
DWS-3160-24PC:admin# disable voice_vlan
Command: disable voice_vlan

Success.
DWS-3160-24PC:admin#
```

81-3 config voice_vlan priority

Description

This command is used to configure the voice VLAN priority value used by this Switch. The voice VLAN priority will be the priority associated with the voice VLAN traffic to distinguish the QoS of the voice traffic from data traffic.

Format

config voice_vlan priority <int 0-7>

Parameters

priority - The priority of the voice VLAN. The default priority is 5.

<int 0-7> - Enter the priority value here. This value must be between 0 and 7.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the priority of the voice VLAN to be six:

```
DWS-3160-24PC:admin# config voice_vlan priority 6
Command: config voice_vlan priority 6

Success.

DWS-3160-24PC:admin#
```

81-4 config voice_vlan oui

Description

This command is used to configure the user-defined voice traffic's OUI. The OUI is used to identify the voice traffic. There are a number of pre-defined OUIs. The user can further define the user-defined OUIs if needed. The user-defined OUI cannot be the same as the pre-defined OUI.

The following are the pre-defined voice traffic's OUI:

OUI	Vendor	Mnemonic name
00:E0:BB	3COM	3com
00:03:6B	Cisco	cisco
00:E0:75	Veritel	veritel
00:D0:1E	Pingtel	pingtel
00:01:E3	Siemens	siemens
00:60:B9	NEC/ Philips	nec&philips
00:0F:E2	Huawei-3COM	huawei&3com
00:09:6E	Avaya	avaya

Format

config voice_vlan oui [add | delete] <macaddr> <macmask> {description <desc 32>}

Parameters

oui - Specifies the OUI used for this configuration. **add** - Adding a user-defined OUI of a voice device vendor. **delete** - Deleting a user-defined OUI of a voice device vendor.
<macaddr> - The user-defined OUI MAC address.
<macmask> - The user-defined OUI MAC address mask.
description - (Optional) The description for the user-defined OUI. **<desc 32>** - Enter the description here. This value can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a user-defined OUI for a voice device:

```
DWS-3160-24PC:admin#config voice_vlan oui add 00-0A-0B-00-00-00 FF-FF-FF-00-00-
00
Command: config voice_vlan oui add 00-0A-0B-00-00-00 FF-FF-FF-00-00-00

Success.

DWS-3160-24PC:admin#
```

81-5 config voice_vlan ports

Description

This command is used to enable or disable the voice VLAN function on ports.

Format

config voice_vlan ports [<portlist> | all] [state [enable | disable] | mode [auto | manual]]

Parameters

ports - Specifies a range of port to set.
- **<portlist>** - Enter a list of ports used for the configuration here.
- **all** - Specifies that all the ports will be used for this configuration.

state - The voice VLAN function state on ports. The default state is disabled.
- **enable** - Specifies that the voice VLAN function for this Switch will be enabled.
- **disable** - Specifies that the voice VLAN function for this Switch will be disabled.

mode - The voice VLAN mode. The default mode is auto.
- **auto** - Specifies that the voice VLAN mode will be set to auto.
- **manual** - Specifies that the voice VLAN mode will be set to manual.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure voice VLAN ports 4-6 to enable:

```
DWS-3160-24PC:admin# config voice_vlan ports 4-6 state enable
Command: config voice_vlan ports 4-6 state enable

Success.

DWS-3160-24PC:admin#
```

To set the mode auto to voice VLAN ports 3-5:

```
DWS-3160-24PC:admin# config voice_vlan ports 3-5 mode auto
Command: config voice_vlan ports 3-5 mode auto

Success.

DWS-3160-24PC:admin#
```

81-6 config voice_vlan aging_time

Description

This command is used to set the aging time of the voice VLAN. The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of the voice VLAN aging timer.

If the voice traffic resumes during the aging time, the aging timer will be stopped and reset.

Format

config voice_vlan aging_time <min 1-65535>

Parameters

aging_time - The aging time to set. The default value is 720 minutes.

<min 1-65535> - Enter the aging time value here. This value must be between 1 and 65535.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set 60 minutes as the aging time of voice VLAN:

```
DWS-3160-24PC:admin# config voice_vlan aging_time 60
Command: config voice_vlan aging_time 60

Success.

DWS-3160-24PC:admin#
```

81-7 show voice_vlan

Description

This command is used to display the voice VLAN global information.

Format

show voice_vlan

Parameters

None.

Restrictions

None.

Example

To display the voice VLAN global information when voice VLAN is enabled:

```
DWS-3160-24PC:admin#show voice_vlan
Command: show voice_vlan

Voice VLAN State     : Enabled
VLAN ID              : 2
VLAN Name            : v2
Priority             : 6
Aging Time           : 60 minutes
Log State            : Enabled
Member Ports         :
Dynamic Member Ports :

DWS-3160-24PC:admin#
```

To display the voice VLAN global information when voice VLAN is disabled:

```
DWS-3160-24PC:admin#show voice_vlan
Command: show voice_vlan

Voice VLAN State     : Disabled
Voice VLAN           : Unassigned
Priority             : 6
Aging Time           : 60 minutes
Log State            : Enabled

DWS-3160-24PC:admin#
```

81-8 show voice_vlan oui

Description

This command is used to display OUI information of voice VLAN.

Format

show voice_vlan oui

Parameters

None.

Restrictions

None.

Example

To display the OUI information of voice VLAN:

```
DWS-3160-24PC:admin#show voice_vlan oui
Command: show voice_vlan oui

OUI Address         Mask               Description
------------------  -----------------  --------------
00-01-E3-00-00-00  FF-FF-FF-00-00-00  Siemens
00-03-6B-00-00-00  FF-FF-FF-00-00-00  Cisco
00-09-6E-00-00-00  FF-FF-FF-00-00-00  Avaya
00-0A-0B-00-00-00  FF-FF-FF-00-00-00
00-0F-E2-00-00-00  FF-FF-FF-00-00-00  Huawei&3COM
00-60-B9-00-00-00  FF-FF-FF-00-00-00  NEC&Philips
00-D0-1E-00-00-00  FF-FF-FF-00-00-00  Pingtel
00-E0-75-00-00-00  FF-FF-FF-00-00-00  Veritel
00-E0-BB-00-00-00  FF-FF-FF-00-00-00  3COM

Total Entries: 9

DWS-3160-24PC:admin#
```

81-9 show voice_vlan ports

Description

This command is used to display the port voice VLAN information.

Format

show voice_vlan ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a list of ports used to be displayed here.	

Restrictions

None.

Example

To display the voice VLAN information of ports 1-5:

```
DWS-3160-24PC:admin#show voice_vlan ports 1-5
Command: show voice_vlan ports 1-5

Ports  Status     Mode
-----  ---------  --------
 1      Disabled   Auto
 2      Disabled   Auto
 3      Disabled   Auto
 4      Enabled    Auto
 5      Enabled    Auto

DWS-3160-24PC:admin#
```

81-10 show voice_vlan voice device

Description

This command is used to display voice devices that are connected to the ports. The start time is the time when the device is detected on this port and the activate time is the latest time the device sent traffic.

Format

show voice_vlan voice_device {ports <portlist>}

Parameters

ports - (Optional) Specifies the list of ports to be configured here.
  <portlist> - Enter a list of ports used to be displayed here.

Restrictions

None.

Example

To display the voice devices that are connected to the ports 1-5:

```
DWS-3160-24PC:admin# show voice_vlan voice_device port 1-5
Command: show voice_vlan voice_device ports 1-5

Ports   Voice Device Address     Start Time    Active Time
-----   --------------------     ---------------     ---------------
1      00-E0-BB-00-00-01   2011-10-6 09:00     2011-10-6 10:30
1      00-E0-BB-00-00-02   2011-10-6 14:10     2011-10-6 15:00
1      00-E0-BB-00-00-03   2011-10-6 14:20     2011-10-6 15:30
2      00-03-6B-00-00-01   2011-10-6 17:15     2011-10-6 18:00
4      00-E0-75-00-00-02   2011-10-6 18:15     2011-10-6 20:00
5      00-01-E3-01-02-03   2011-10-6 18:30     2011-10-6 20:30

Total Entries: 6

DWS-3160-24PC:admin#
```

81-11 config voice_vlan log state

Description

This command is used to configure the log state for voice VLAN. If there is a new voice device detected/or a port joins/leaves the voice VLAN dynamically, and the log is enabled, a log will be triggered.

Format

config voice_vlan log state [enable | disable]

Parameters

log - Specifies to enable or disable the sending of a voice VLAN log.
  enable - Specifies that the sending of a voice VLAN log will be enabled.
  disable - Specifies that the sending of a voice VLAN log will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the log state for voice VLAN:

```
DWS-3160-24PC:admin# config voice_vlan log enable
Command: config voice_vlan log enable

Success.

DWS-3160-24PC:admin#
```

Chapter 82 Wireless Access Point Profile Command List

create wireless ap_profile <int 1-16>

create wireless ap_profile copy <int 1-16> <int 1-16>

delete wireless ap_profile <int 1-16>

config wireless ap_profile <int 1-16> [apply | clear | hwtype [any | hw_dwl8600 | hw_dwl3600 | hw_dwl6600] | name <name 32> | vlan [<int 0-4094> | default] | disconnected_ap [forwarding_mode [enable | disable] | management_mode [enable | disable]] | radio <int 1-2> [uapsd [enable | disable] | beacon_interval [<int 20-2000> | default] | channel [auto [enable | disable] | auto_eligible [add [<int> | all] | delete [<int> | all]]] | dot11n [channel_bandwidth [20 | 40] | primary_channel [lower | upper | default] | short_guard_interval [enable | disable | default] | stbc_mode [enable | disable | default]] | dtim_period [<int 1-255> | default] | status [enable | disable] | fragmentation_threshold [<int 256-2346> | default] | incorrect_frame_no_ack [enable | disable] | load_balance [state [enable | disable] | utilization [<int 1-100> | default]] | mcs_index [add [<int 0-15> | all] | delete [<int 0-15> | all]] | max_clients [<int 0-200> | default] | mode [a | a_n | bg | bg_n | n_only_a | n_only_g | default] | multicast tx_rate <float> | power [auto [enable | disable] | default_power [<int 1-100> | default]] | protection [auto | off | default] | qos [ap_edca [background | best_effort | video | voice] [aifs [<int 1-255> | default] | cwmax [1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 |1023 | default] | cwmin [1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023 | default] | max_burst [<int 0-999900> | default]] | station_edca [background | best_effort | video | voice] [aifs [<int 1-255> | default] | cwmax [1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023 | default] | cwmin [1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023 | default] | txop_limit [<int 0-65535> | default]] | edca template [custom | default | voice]] | rate [basic [add <float> | delete <float>] | supported [add <float> | delete <float>]] | rate_limit [state [enable | disable] | burst [<int 1-75> | default] | normal [<int 1-50> | default]] | rf_scan [duration [<int 10-2000> | default] | other_channel [mode [enable | disable] | interval [<int 30-120> | default]] | sentry [mode [enable | disable] | channels [an | all | bgn | default]]] | rts_threshold [<int 0-2347> | default] | station_isolation [enable | disable] | vap <int 0-15> [state [enable | disable] | network <int 1-64>] | wmm [enable | disable]]]

show wireless ap_profile {<int 1-16> {radio {<int 1-2> {[auto_eligible | mcs_index | qos {[ap_edca | station_edca]} | rates {[basic | supported]} | vap {<int 0-15>}]}}}}

82-1 create wireless ap_profile

Description

This command is used to create an new AP profile.

Format

create wireless ap_profile <int 1-16>

Parameters

<int 1-16> - Enter the new AP profile ID used here. This value must be between 1 and 16.

Restrictions

Only Administrators can issue this command.

Example

To create an new AP profile:

```
DWS-3160-24TC:admin#create wireless ap_profile 2
Command: create wireless ap_profile 2

 Create AP Profile ID : 2

Success.

DWS-3160-24PC:admin#
```

82-2 create wireless ap_profile copy

Description

This command is used to create a copy of an entire existing AP profile. If the destination profile does not exist, it will be created.

Format

create wireless ap_profile copy <int 1-16> <int 1-16>

Parameters

<int 1-16> - Enter the source AP Profile ID here. This value must be between 1 and 16.

<int 1-16> - Enter the destination AP Profile ID here. This value must be between 1 and 16.

Restrictions

Only Administrators can issue this command.

Example

To create a copy of an entire existing AP profile:

```
DWS-3160-24TC:admin#show wireless ap_profile
Command: show wireless ap_profile

AP Profile ID  Profile Name                      Profile Status
-------------  --------------------------------  -------------------
1              Default                           Configured
2              approfile_2                       Configured

Total Entries : 2

DWS-3160-24TC:admin#create wireless ap_profile copy 1 3
Command: create wireless ap_profile copy 1 3

Success.

DWS-3160-24TC:admin#create wireless ap_profile copy 1 2
Command: create wireless ap_profile copy 1 2

Are you sure you want to overwrite the existing profile? (y/n) y
 AP Profile Configuration Copy Successful.

Success.

DWS-3160-24TC:admin#show wireless ap_profile
Command: show wireless ap_profile

AP Profile ID  Profile Name                      Profile Status
-------------  --------------------------------  -------------------
1              Default                           Configured
2              Default                           Configured
3              Default                           Configured

Total Entries : 3

DWS-3160-24TC:admin#
```

82-3 delete wireless ap_profile

Description

This command is used to delete an AP profile. If the profile is referenced by an entry in the valid AP database, or is applied to one or more managed APs, it cannot be deleted. The default profile (1 – Default) can never be deleted.

Format

delete wireless ap_profile <int 1-16>

Parameters

<int 1-16> - Enter the AP profile ID, that will be deleted, here. This value must be between 1 and 16.

Restrictions

Only Administrators can issue this command.

Example

To delete the AP Profile with ID 5:

```
DWS-3160-24PC:admin#delete wireless ap_profile 5
Command: delete wireless ap_profile 5

 Delete AP Profile ID : 5

Success.

DWS-3160-24PC:admin#
```

82-4 config wireless ap_profile

Description

This command is used to configure an wireless access point profile. Access point profiles can be applied to multiple physical APs.

Format

config wireless ap_profile <int 1-16> [apply | clear | hwtype [any | hw_dwl8600 | hw_dwl3600 | hw_dwl6600] | name <name 32> | vlan [<int 0-4094> | default] | disconnected_ap [forwarding_mode [enable | disable] | management_mode [enable | disable]] | radio <int 1-2> [uapsd [enable | disable] | beacon_interval [<int 20-2000> | default] | channel [auto [enable | disable] | auto_eligible [add [<int> | all] | delete [<int> | all]]] | dot11n [channel_bandwidth [20 | 40] | primary_channel [lower | upper | default] | short_guard_interval [enable | disable | default] | stbc_mode [enable | disable | default]] | dtim_period [<int 1-255> | default] | status [enable | disable] | fragmentation_threshold [<int 256-2346> | default] | incorrect_frame_no_ack [enable | disable] | load_balance [state [enable | disable] | utilization [<int 1-100> | default]] | mcs_index [add [<int 0-15> | all] | delete [<int 0-15> | all]] | max_clients [<int 0-200> | default] | mode [a | a_n | bg | bg_n | n_only_a | n_only_g | default] | multicast tx_rate <float> | power [auto [enable | disable] | default_power [<int 1-100> | default]] | protection [auto | off | default] | qos [ap_edca [background | best_effort | video | voice] [aifs [<int 1-255> | default] | cwmax [1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 |1023 | default] | cwmin [1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023 | default] | max_burst [<int 0-999900> | default]] | station_edca [background | best_effort | video | voice] [aifs [<int 1-255> | default] | cwmax [1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023 | default] | cwmin [1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023 | default] | txop_limit [<int 0-65535> | default]] | edca template [custom | default | voice]] | rate [basic [add <float> | delete <float>] | supported [add <float> | delete <float>]] | rate_limit [state [enable | disable] | burst [<int 1-75> | default] | normal [<int 1-50> | default]] | rf_scan [duration [<int 10-2000> | default] | other_channel [mode [enable | disable] | interval [<int 30-120> | default]] | sentry [mode [enable | disable] | channels [an | all | bgn | default]]] | rts_threshold [<int 0-2347> | default] | station_isolation [enable | disable] | vap <int 0-15> [state [enable | disable] | network <int 1-64>] | wmm [enable | disable]]]

Parameters

<int 1-16> - Enter the wireless AP Profile ID used here. This value must be between 1 and 16.

apply - Specifies to resend the AP profile configuration to all managed APs associated with the profile. This allows you to apply configuration changes to the APs that are already managed.

clear - Specifies to restores an AP profile configuration to its default values, except for the profile name. The profile name is not an AP configuration and is only used for descriptive purposes.

hwtype - Specifies to configure the AP hardware type. The hardware type is determined, in part, by the number of radios the AP supports (single or dual) and the IEEE 802.11 modes that the radio supports.

- **Any** - Specifies a general AP hardware type. Dual Radio 802.11a/b/g/n.
- **hw_dwl8600** - Specifies that the AP hardware type is a DWL-8600AP, Dual Radio 802.11a/b/g/n.
- **hw_dwl3600** - Specifies that the AP hardware type is a DWL-3600AP, Single Radio 802.11b/g/n.
- **hw_dwl6600** - Specifies that the AP hardware type is a DWL-6600AP, Dual Radio 802.11a/b/g/n.

name - Specifies the descriptive name for the AP Profile.

- **<name 32>** - Enter the descriptive name for the AP Profile here. This name can be up to 32 characters long.

vlan - Specifies the VLAN ID used to send tracer packets using the wired network detection algorithm. If VLAN ID is '0', then tracer packets will be sent untagged.

- **<int 0-4094>** - Enter the VLAN ID used to send tracer packets using the wired network detection algorithm here. This value must be between 0 and 4094. The default value is 1.
- **default** - Specifies that the default option will be used.

disconnected_ap - Specifies the behavior of an AP when it disconnects.

- **forwarding_mode** - Specifies to configure the AP's forwarding mode state. This also specifies whether the managed AP should allow clients that are already associated to continue forwarding traffic when the AP loses connection with the wireless Switch. If this field is disabled, the AP will not allow clients to forward data if the AP loses its connection with the Switch that is managing it.
  - **enable** - Specifies that the AP's forwarding mode will be enabled.
  - **disable** - Specifies that the AP's forwarding mode will be disabled. This is the default option.
- **management_mode** - Specifies to configure the AP's management mode state. This also specifies whether the managed AP should enable the stand-alone management functionality when it loses connection with the wireless Switch. If this field is disabled, the AP will not allow TELNET, Web, or SNMP access to the stand-alone management interface.
  - **enable** - Specifies that the AP's management mode will be enabled. This is the default option.
  - **disable** - Specifies that the AP's management mode will be disabled.

radio - Specifies the RF configuration for a radio interface within an access point profile.

- **<int 1-2>** - Enter the RF configuration value for a radio interface within an access point profile here. This value must be between 1 and 2.
- **uapsd** - Specifies the state of the automatic power save delivery mode for the radio.
  - **enable** - Specifies that the automatic power save delivery mode for the radio will be enabled. This is the default option.
  - **disable** - Specifies that the automatic power save delivery mode for the radio will be disabled.
- **beacon_interval** - Specifies the beacon interval for the radio. The beacon interval indicates the interval at which the AP radio transmits beacon frames.
  - **<int 20-2000>** - Enter the beacon interval value for the radio here. This value must be between 20 and 2000 milliseconds. The default value is 100 milliseconds.
  - **default** - Specifies that the default value will be used.
- **channel auto** - Specifies the automatic channel adjustment for the radio. This indicates that the initial AP channel assignment can be automatically adjusted by the Switch.
  - **enable** - Specifies that the automatic channel adjustment feature will be enabled.
  - **disable** - Specifies that the automatic channel adjustment feature will be disabled. This is the default option.

auto_eligible - Specifies to enable either one or all of the supported channels on the radio to be eligible for auto-channel selection. If you Specifies one channel, the command will succeed only if this channel is supported by the current mode of the radio. If 'all' is chosen, then all channels supported by the current radio mode will be enabled for automatic selection.

add - Specifies to add a channel in the automatic eligible group.

<int> - Enter the automatic eligible channel number that will be added here.

all - Specifies that all the available channels will be added to the automatic eligible group. This is the default option.

delete - Specifies to delete a channel from the automatic eligible group.

<int> - Enter the automatic eligible channel number that will be deleted here.

all - Specifies that all the channels will be removed from the automatic eligible group.

dot11n - Specifies that parameters regarding the 802.11n channel bandwidth will be configured.

channel_bandwidth - Specifies the bandwidth used by the channel when operating in 802.11n mode.

20 - Specifies the radio will operate in the 20MHz bandwidth.

40 - Specifies the radio will operate in the 40MHz bandwidth. This is the default option.

primary_channel - Specifies the bandwidth used by the channel when operating in 802.11n mode.

lower - Specifies that the relative location of the primary channel will be on the lower side in the 40 MHz channel. This is the default option.

upper - Specifies that the relative location of the primary channel will be on the upper side in the 40 MHz channel.

default - Specifies that the default option will be used.

short_guard_interval - Specifies the short guard interval's state, when operating in 802.11n mode.

enable - Specifies that the short guard interval will be enabled. The guard interval value is set as 400ns. This is the default option.

disable - Specifies that the short guard interval will be disabled. The guard interval value is set as 800ns.

default - Specifies that the default option will be used.

stbc_mode - Specifies the Space Time Block Code (STBC) mode when operating in 802.11n mode. The STBC enables the AP to send the same data stream on multiple antennas at the same time.

enable - Specifies to send the same data stream on multiple antennas at the same time. This is the default option.

disable - Specifies to divide the same data stream between two antennas.

default - Specifies that the default option will be used.

dtim_period - Specifies the DTIM period for the radio. The DTIM period is the number of beacons between DTIMs. A DTIM is Delivery Traffic Indication Map which indicates there is buffered broadcast or multicast traffic on the AP.

<int 1-255> - Enter the DTIM period value used here. This value must be between 1 and 255. The default value is 10 beacons.

default - Specifies that the default value will be used.

status - Specifies the administrative mode of the radio interface to the ‘on' state.

enable - Specifies that the administrative mode of the radio interface to the 'on' state will be enabled. This is the default option.

disable - Specifies that the administrative mode of the radio interface to the 'on' state will be disabled.

fragmentation_threshold - Specifies the fragmentation threshold for the radio. The fragmentation threshold indicates a limit on the size of packets that can be fragmented. A threshold of 2346 indicates that there should be no fragmentation.

<int 256-2346> - Enter the fragmentation threshold value used here. This value must be between 256 and 2346. The default value is 2346.

default - Specifies that the default value will be used.

incorrect_frame_no_ack - Specifies whether or not to send any acknowledgements for incorrectly received frames.

enable - Specifies not to send any acknowledgements for incorrectly received frames. This is the default option.

disable - Specifies to send any acknowledgements for incorrectly received frames.

load_balance - Specifies that the load balancing feature will be configured.

state - Specifies the load balancing state.

enable - Specifies that the load balancing feature will be enabled.

disable - Specifies that the load balancing feature will be enabled. This is the default option.

utilization - Specifies the percentage of network utilization allowed on the radio before clients are denied.

<int 1-100> - Enter the network utilization value here. This value must be between 1 and 100. This unit is in percentage. The default value is 60%.

default - Specifies that the default value will be used.

mcs_index - Specifies that the MCS Index feature will be configured.

add - Specifies to add an MCS Index when operating in 802.11n mode.

<int 0-15> - Enter the MCS Index value, that will be added, here. This value must be between 0 and 15.

all - Specifies that all the values will be added to the MCS Index value.

delete - Specifies to delete an MCS Index when operating in 802.11n mode.

<int 0-15> - Enter the MCS Index value, that will be deleted, here. This value must be between 0 and 15.

all - Specifies that all the values will be deleted from the MCS Index value.

max_clients - Specifies the maximum number of simultaneous client associations allowed on the radio interface.

<int 0-200> - Enter the maximum number of simultaneous client associations here. This value must be between 0 and 200. The default value is 200.

default - Specifies that the default value will be used.

mode - Specifies the physical layer technology to use on the radio.

a - Specifies that 802.11a will be used in the physical mode.

a_n - Specifies that 802.11a/n will be used in the physical mode.

bg - Specifies that 802.11b/g will be used in the physical mode.

bg_n - Specifies that 802.11b/g/n will be used in the physical mode. This option is only available for Radio 2.

n_only_a - Specifies that 802.11n, in the 5GHz band, will be used in the physical mode. This option is only available for Radio 1.

n_only_g - Specifies that 802.11n, in the 2.4GHz band, will be used in the physical mode. This option only available for Radio 2.

default - Specifies that the default option will be used. The default option for Radio 1 is 802.11a/n. The default option for Radio 2 is 802.11b/g/n.

multicast - Specifies the rate at which the radio transmits multicast frames.

tx_rate - Specifies the TX rate at which the radio transmits multicast frames.

<float> - Enter a valid rate, based on the radio mode, here. When the radio is operating in the 5 GHz band, available values are 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. When the radio is operating in the 2.4 GHz band, available values are 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps. When this value is set to 0, the multicast transmission rate selection is automatic.

power - Specifies the state of the automatic power adjustment feature, for the radio.

auto - Specifies that the AP power assignment can automatically be adjusted by the Switch.

enable - Specifies that the automatic power adjustment feature will be enabled.

disable - Specifies that the automatic power adjustment feature will be disabled.

default_power - Specifies to configure the power setting for the radio. When the automatic power adjustment feature is enabled, an initial default power setting will be used. Alternatively, a fixed power setting will be used. The automatic power algorithm will not reduce the power below the number you set in the default power field. By default, the power level is 100%. Even if you enable the automatic power feature, the power of the RF signal will not decrease. The power level is a percentage of the maximum transmission power for the RF signal.

<int 1-100> - Enter the default power settings value here. This value must be between 1 and 100. The default value is 100.

default - Specifies that the default value will be used.

protection - Specifies the protection mode to use when operating in 802.11n mode. When the protection mode is enabled, APs and stations will ensure that transmission is protected if there are legacy stations using the same radio frequency.

auto - Specifies that the protection mechanism is set to the “automatic” mode. This is the default option.

off - Specifies that the protection mechanism is set to the “off” mode.

default - Specifies that the default option will be used.

qos ap_edca - Specifies that the downstream traffic flowing from the access point to the client station EDCA queues for Voice (0), Video (1), Best-effort (2), and Background (3) queues. The user can configure the AIFS (Arbitration Inter-Frame Spacing), Minimum Contention Window, Maximum Contention Window, and the Maximum Burst Duration for each of these queues.

background - Specifies that the AIFS will be set as 7ms, the Minimum Contention Window as 15ms, the Maximum Contention Window as 1023ms, and the Maximum Burst Duration as 0µs.

best_effort - Specifies that the AIFS will be set as 3ms, the Minimum Contention Window as 15ms, the Maximum Contention Window as 63msecs, and the Maximum Burst Duration as 0µs.

video - Specifies that the AIFS will be set as 1ms, the Minimum Contention Window as 7ms, the Maximum Contention Window as 15ms, and the Maximum Burst Duration as 3000µs.

voice - Specifies that the AIFS will be set as 1ms, the Minimum Contention Window as 3ms, the Maximum Contention Window as 7ms, and the Maximum Burst Duration as 1500µs.

aifs - Specifies that the Arbitration Inter-Frame Spacing (AIFS) will be configured.

<int 1-255> - Enter the AIFS value used here. This value must be between 1 and 255.

default - Specifies that the default value will be used.

cwmax - Specifies to configure the Maximum Contention Window value in milliseconds.

1 - Specifies that the Maximum Contention Window value will be set as 1ms.

3 - Specifies that the Maximum Contention Window value will be set as 3ms.

7 - Specifies that the Maximum Contention Window value will be set as 7ms.

15 - Specifies that the Maximum Contention Window value will be set as 15ms.

31 - Specifies that the Maximum Contention Window value will be set as 31ms.

63 - Specifies that the Maximum Contention Window value will be set as 63ms.

127 - Specifies that the Maximum Contention Window value will be set as 127ms.

255 - Specifies that the Maximum Contention Window value will be set as 255ms.

511 - Specifies that the Maximum Contention Window value will be set as 511ms.

1023 - Specifies that the Maximum Contention Window value will be set as 1023ms.

default - Specifies that the default value will be used.

cwmin - Specifies to configure the Minimum Contention Window value in milliseconds.

1 - Specifies that the Minimum Contention Window value will be set as 1ms.

3 - Specifies that the Minimum Contention Window value will be set as 3ms.

7 - Specifies that the Minimum Contention Window value will be set as 7ms.

15 - Specifies that the Minimum Contention Window value will be set as 15ms.

31 - Specifies that the Minimum Contention Window value will be set as 31ms.

63 - Specifies that the Minimum Contention Window value will be set as 63ms.

127 - Specifies that the Minimum Contention Window value will be set as 127ms.

255 - Specifies that the Minimum Contention Window value will be set as 255ms.

511 - Specifies that the Minimum Contention Window value will be set as 511ms.

1023 - Specifies that the Minimum Contention Window value will be set as 1023ms.

default - Specifies that the default value will be used.

max_burst - Specifies to configure the Maximum Burst Duration value in microseconds. (µs)

<int 0-999900> - Enter the Maximum Burst Duration value used here. This value must be between 0 and 999900µs.

default - Specifies that the default value will be used.

station_edca - Specifies that the upstream traffic flowing from the client station to the access point EDCA queues for voice (0), video (1), best-effort (2), and background (3) queues. The user can configure the AIFS (Arbitration Inter-Frame Spacing), Minimum Contention Window, Maximum Contention Window, and the Transmission Opportunity Limit for each of these queues.

background - Specifies that the AIFS will be set as 7ms, the Minimum Contention Window as 15ms, the Maximum Contention Window as 1023ms, and the Transmission Opportunity Limit as 0ms.
best_effort - Specifies that the AIFS will be set as 3ms, the Minimum Contention Window as 15ms, the Maximum Contention Window as 1023ms, and the Transmission Opportunity Limit as 0ms.
video - Specifies that the AIFS will be set as 2ms, the Minimum Contention Window as 7ms, the Maximum Contention Window as 15ms, and the Transmission Opportunity Limit as 94ms.
voice - Specifies that the AIFS will be set as 3ms, the Minimum Contention Window as 3ms, the Maximum Contention Window as 7ms, and the Transmission Opportunity Limit as 47ms.
aifs - Specifies that the Arbitration Inter-Frame Spacing (AIFS) will be configured.
<int 1-255> - Enter the AIFS value used here. This value must be between 1 and 255.
default - Specifies that the default value will be used.
cwmax - Specifies to configure the Maximum Contention Window value in milliseconds.
1 - Specifies that the Maximum Contention Window value will be set as 1ms.
3 - Specifies that the Maximum Contention Window value will be set as 3ms.
7 - Specifies that the Maximum Contention Window value will be set as 7ms.
15 - Specifies that the Maximum Contention Window value will be set as 15ms.
31 - Specifies that the Maximum Contention Window value will be set as 31ms.
63 - Specifies that the Maximum Contention Window value will be set as 63ms.
127 - Specifies that the Maximum Contention Window value will be set as 127ms.
255 - Specifies that the Maximum Contention Window value will be set as 255ms.
511 - Specifies that the Maximum Contention Window value will be set as 511ms.
1023 - Specifies that the Maximum Contention Window value will be set as 1023ms.
default - Specifies that the default value will be used.
cwmin - Specifies to configure the Minimum Contention Window value in milliseconds.
1 - Specifies that the Minimum Contention Window value will be set as 1ms.
3 - Specifies that the Minimum Contention Window value will be set as 3ms.
7 - Specifies that the Minimum Contention Window value will be set as 7ms.
15 - Specifies that the Minimum Contention Window value will be set as 15ms.
31 - Specifies that the Minimum Contention Window value will be set as 31ms.
63 - Specifies that the Minimum Contention Window value will be set as 63ms.
127 - Specifies that the Minimum Contention Window value will be set as 127ms.
255 - Specifies that the Minimum Contention Window value will be set as 255ms.
511 - Specifies that the Minimum Contention Window value will be set as 511ms.
1023 - Specifies that the Minimum Contention Window value will be set as 1023ms.
default - Specifies that the default value will be used.
txop_limit - Specifies to configure the Transmission Opportunity Limit value in milliseconds.
<int 0-65535> - Enter the Transmission Opportunity Limit value used here. This value must be between 0 and 65535ms.
default - Specifies that the default value will be used.
edca template - Specifies whether the EDCA parameters are set to one of the predefined templates or manually configured. If the user selects 'custom', then the user can change the AP and station parameters. If user selects 'voice' or 'default', then the Switch will use the pre-defined settings for the template selected.
custom - Specifies that the custom EDCA template will be used.
default - Specifies that the default EDCA template will be used.
voice - Specifies that the voice EDCA template will be used.
rate - Specifies that the client data rates, for the radio, will be configured.
basic - Specifies to configure the list of basic client data rates for the radio. The basic rates are the list of data rates that all stations associating with the AP must support.
add - Specifies to add a basic data rate to the corresponding list.
<float> - Enter a valid data rate, in Mbps, here based on the radio mode.
delete - Specifies to delete a basic data rate from the corresponding list.
<float> - Enter a valid data rate, in Mbps, here based on the radio mode.
supported - Specifies to configure the list of supported client data rates for the radio. The supported rates are those the AP will allow when setting up communications with client

stations.

add - Specifies to add a supported data rate to the corresponding list.

<float> - Enter a valid data rate, in Mbps, here based on the radio mode.

delete - Specifies to delete a supported data rate from the corresponding list.

<float> - Enter a valid data rate, in Mbps, here based on the radio mode.

rate_limit - Specifies that enabling the multicast and broadcast rate limitation can improve overall network performance by limiting the number of packets transmitted across the network.

state - Specifies the broadcast and multicast traffic rate limitation's state on the radio.

enable - Specifies that the broadcast and multicast traffic rate limitation's state on the radio will be enabled.

disable - Specifies that the broadcast and multicast traffic rate limitation's state on the radio will be disabled. This is the default value.

burst - Specifies to configure the burst traffic rate. Traffic can occur in bursts up to this value before all traffic is considered to exceed the limit.

<int 1-75> - Enter the burst traffic rate value used here. This value must be between 1 and 75 packets per second. The default value is 75 packets per second.

default - Specifies that the default value will be used.

normal - Specifies to configure the rate limit for normal traffic. All traffic below this limit is transmitted.

<int 1-50> - Enter the rate limit for normal traffic used here. This value must be between 1 and 50 packets per second. The default value is 50 packets per second.

default - Specifies that the default value will be used.

rf_scan - Specifies that the FR scan feature will be configured.

duration - Specifies the RF scan duration for the radio. The duration indicates how long the radio will scan on one channel.

<int 10-2000> - Enter the RF scan duration value used here. This value must be between 10 and 2000ms. The default value is 10ms.

default - Specifies that the default value will be used.

other_channel - Specifies that the access point can perform RF scans to collect information about other wireless devices within range and then report this information to the UWS.

mode - Specifies to enable or disable the radio to perform RF scanning on channels other than its operating channel.

enable - Specifies that the radio will perform RF scanning on channels other than its operating channel. This is the default option.

disable - Specifies that the radio will not perform RF scanning on channels other than its operating channel.

interval - Specifies how often the radio will leave its operational channel.

<int 30-120> - Enter the interval value used here. This value must be between 30 and 120 seconds. The default value is 60 seconds.

default - Specifies that the default value will be used.

sentry - Specifies that when the RF Scan Sentry option is enabled, the radio primarily performs dedicated RF scanning. The radio passively listens for beacons and traffic exchanges between clients and other access points but does not accept connections from wireless clients. In sentry mode, all VAPs are disabled. Networks that deploy sentry APs or radios can detect devices on the network quicker and perform a more thorough security analysis. In this mode, the radio Switches from one channel to the next. The length of time spent on each channel is controlled by the scan duration. The default scan duration is 10 milliseconds.

mode - Specifies whether to enable or disable dedicated RF scanning and normal operation of the radio. The radio will not allow any client associations when sentry mode is enabled.

enable - Specifies that the sentry mode will be enabled.

disable - Specifies that the sentry mode will be disabled. This is the default option.

channels - Specifies to scan channels within the specified mode or frequency.

an - Specifies to perform an RF scan on all 802.11a/n channels on the 5GHz frequency.

all - Specifies to perform an RF scan on all the channels. This is the default option.

bgn - Specifies to perform an RF scan on all 802.11b/g/n channels on the 2.4GHz frequency.

default - Specifies that the default option will be used.

rts_threshold - Specifies the RTS threshold for the radio. This indicates the number of octets in an MPDU, below which an RTS/CTS handshake shall not be performed.

<int 0-2347> - Enter the RTS threshold value used here. This value must be between 0 and 2347. The default value is 2347.

default - Specifies that the default value will be used.

station_isolation - Specifies whether to enable or disable the Station Isolation mode on the radio. When Station Isolation is enabled, the access point blocks communication between wireless clients. The access point still allows data traffic between its wireless clients and wired devices on the network, but not among wireless clients.

enable - Specifies that the Station Isolation mode, on the radio, will be enabled.

disable - Specifies that the Station Isolation mode, on the radio, will be disabled. This is the default option.

vap - Specifies the Virtual Access Point (VAP) configuration, per radio interface, within an access point profile.

<int 0-15> - Enter the VAP value used here. This value must be between 0 and 15.

state - Specifies whether to enable or disable the configured VAP on the radio. VAP0 cannot be disabled. If you want to disable VAP0, you must turn off the radio option.

enable - Specifies that the configured VAP, on the radio, will be enabled.

disable - Specifies that the configured VAP, on the radio, will be disabled. This is the default option.

network - Specifies the network to apply to the VAP. A VAP must be configured with a network.

<int 1-64> - Enter the network ID used here. This value must be between 1 and 64.

wmm - Specifies whether to enable or disable the WMM mode for the radio. WMM mode is known as Wi-Fi Multimedia mode. When enabled the QoS settings it'll affect both the downstream traffic to the station (AP EDCA parameters) and the upstream traffic to the AP (station EDCA parameters). When disabled, the QoS will only be applied to the downstream traffic.

enable - Specifies that the WWM mode, for the radio, will be enabled. This is the default option.

disable - Specifies that the WWM mode, for the radio, will be disabled.

Restrictions

Only Administrators can issue this command.

Example

To apply an AP Profile to a WS Managed APs associated with the AP Profile:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 apply
Command: config wireless ap_profile 1 apply
Do you want to apply the configuration to all managed APs associated with this
profile? (y/n) y
 AP Profile apply is in progress.

Success.

DWS-3160-24PC:admin#
```

To restore AP Profile 1’s configuration to the default values:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 clear
Command: config wireless ap_profile 1 clear

All configurations will be set to the default values for this profile
 except the profile name. Are you sure you want to clear the profile
 configuration? (y/n) y
 Clear the AP Profile Configuration.

Success.

DWS-3160-24PC:admin#
```

To configure the AP hardware type on AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 hwtype any
Command: config wireless ap_profile 1 hwtype any

Success.

DWS-3160-24PC:admin#
```

To configure the profile name on AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 name approfile
Command: config wireless ap_profile 1 name approfile

Success.

DWS-3160-24PC:admin#
```

To configure the VLAN on AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 vlan 3
Command: config wireless ap_profile 1 vlan 3

Success.

DWS-3160-24PC:admin#
```

To enable the Disconnected-AP Forwarding Mode on AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 disconnected_ap
forwarding_mode enable
Command: config wireless ap_profile 1 disconnected_ap forwarding_mode enable

Success.

DWS-3160-24PC:admin#
```

To enable the Disconnected-AP Management Mode on AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 disconnected_ap
management_mode enable
Command: config wireless ap_profile 1 disconnected_ap management_mode enable

Success.

DWS-3160-24PC:admin#
```

To enable the automatic power save delivery (uapsd) mode on radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 uapsd enable
Command: config wireless ap_profile 1 radio 1 uapsd enable

Success.

DWS-3160-24PC:admin#
```

To configure the beacon interval on radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 beacon_interval 200
Command: config wireless ap_profile 1 radio 1 beacon_interval 200

Success.

DWS-3160-24PC:admin#
```

To enable auto channel adjustment for the radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 channel auto enable
Command: config wireless ap_profile 1 radio 1 channel auto enable

Success.

DWS-3160-24PC:admin#
```

To enable all of the supported channels on the radio 1 of AP Profile 1 to be eligible for auto-channel selection:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 channel auto_eligible
add all
Command: config wireless ap_profile 1 radio 1 channel auto_eligible add all

Success.

DWS-3160-24PC:admin#
```

To configure the bandwidth used in the channel when operating in 802.11n mode:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 dot11n
channel_bandwidth 20
Command: config wireless ap_profile 1 radio 1 dot11n channel_bandwidth 20

Success.

DWS-3160-24PC:admin#
```

To enable the short guard interval when operating in 802.11n mode:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 dot11n
short_guard_interval enable
Command: config wireless ap_profile 1 radio 1 dot11n short_guard_interval
enable

Success.

DWS-3160-24PC:admin#
```

To enable the Space Time Block Code (STBC) Mode on radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 dot11n stbc_mode
enable
Command: config wireless ap_profile 1 radio 1 dot11n stbc_mode enable

Success.

DWS-3160-24PC:admin#
```

To configure the DTIM period for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 dtim_period 100
Command: config wireless ap_profile 1 radio 1 dtim_period 100

Success.

DWS-3160-24PC:admin#
```

To enable the administrative mode of the radio interface (Radio 1) on AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 status enable
Command: config wireless ap_profile 1 radio 1 status enable

Success.

DWS-3160-24PC:admin#
```

To configure the fragmentation threshold for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1
fragmentation_threshold 2312
Command: config wireless ap_profile 1 radio 1 fragmentation_threshold 2312

Success.

DWS-3160-24PC:admin#
```

To enable the incorrect-frame-no-ack for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 incorrect_frame_no_ack
enable
Command: config wireless ap_profile 1 radio 1 incorrect_frame_no_ack enable

Success.

DWS-3160-24PC:admin#
```

To enable load balancing for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 load_balance state
enable
Command: config wireless ap_profile 1 radio 1 load_balance state enable

Success.

DWS-3160-24PC:admin#
```

To configure the utilization parameter of load balancing for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 load_balance
utilization 60
Command: config wireless ap_profile 1 radio 1 load_balance utilization 60

Success.

DWS-3160-24PC:admin#
```

To add an MCS Index for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 mcs_index add 2
Command: config wireless ap_profile 1 radio 1 mcs_index add 2

Success.

DWS-3160-24PC:admin#
```

To delete an MCS Index for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 mcs_index delete 3
Command: config wireless ap_profile 1 radio 1 mcs_index delete 3

Success.

DWS-3160-24PC:admin#
```

To configure the maximum number of simultaneous clients for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 max_clients 100
Command: config wireless ap_profile 1 radio 1 max_clients 100

Success.

DWS-3160-24PC:admin#
```

To configure the Multicast TX-Rate for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 multicast tx_rate 9
Command: config wireless ap_profile 1 radio 1 multicast tx_rate 9

Success.

DWS-3160-24PC:admin#
```

To enable the auto power adjustment for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 power auto enable
Command: config wireless ap_profile 1 radio 1 power auto enable

Success.

DWS-3160-24PC:admin#
```

To configure the power setting of the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 power default_power 60
Command: config wireless ap_profile 1 radio 1 power default_power 60

Success.

DWS-3160-24PC:admin#
```

To configure the protection mode for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 protection auto
Command: config wireless ap_profile 1 radio 1 protection auto

Success.

DWS-3160-24PC:admin#
```

To configure the parameters of QoS AP-EDCA queues (including voice, video, best-effort and background queues) for the Radio 1 of AP Profile 1. The parameters include AIFS, Minimum Contention Window, Maximum Contention Window, and Maximum Burst Duration.

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 qos ap_edca video aifs
11
Command: config wireless ap_profile 1 radio 1 qos ap_edca video aifs 11

Success.

DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 qos ap_edca video
cwmax 7
Command: config wireless ap_profile 1 radio 1 qos ap_edca video cwmax 7

Success.

DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 qos ap_edca video
cwmin 3
Command: config wireless ap_profile 1 radio 1 qos ap_edca video cwmin 3

Success.

DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 qos ap_edca video
max_burst 11
Command: config wireless ap_profile 1 radio 1 qos ap_edca video max_burst 11

Success.

DWS-3160-24PC:admin#
```

To configure the parameters of QoS Station-EDCA queues (including voice, video, best-effort and background queues) for the Radio 1 of AP Profile 1. The parameters include AIFS, Minimum Contention Window, Maximum Contention Window, and Transmission Opportunity

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 qos station_edca voice
aifs 22
Command: config wireless ap_profile 1 radio 1 qos station_edca voice aifs 22

Success.

DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 qos station_edca voice
cwmax 15
Command: config wireless ap_profile 1 radio 1 qos station_edca voice cwmax 15

Success.

DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 qos station_edca voice
cwmin 7
Command: config wireless ap_profile 1 radio 1 qos station_edca voice cwmin 7

Success.

DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 qos station_edca voice
txop_limit 222
Command: config wireless ap_profile 1 radio 1 qos station_edca voice txop_limit
222

Success.

DWS-3160-24PC:admin#
```

To configure the list of basic client data rates for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 rate basic add 9
Command: config wireless ap_profile 1 radio 1 rate basic add 9

Success.

DWS-3160-24PC:admin#
```

To configure the list of supported client data rates for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 rate supported add 18
Command: config wireless ap_profile 1 radio 1 rate supported add 18

Success.

DWS-3160-24PC:admin#
```

To enable broadcast and multicast traffic rate limiting for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 rate_limit state
enable
Command: config wireless ap_profile 1 radio 1 rate_limit state enable

Success.

DWS-3160-24PC:admin#
```

To configure normal and burst traffic rate limiting for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 rate_limit burst 30
Command: config wireless ap_profile 1 radio 1 rate_limit burst 30

Success.

DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 rate_limit normal 20
Command: config wireless ap_profile 1 radio 1 rate_limit normal 20

Success.

DWS-3160-24PC:admin#
```

To configure the RF scan duration for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 rf_scan duration 1000
Command: config wireless ap_profile 1 radio 1 rf_scan duration 1000

Success.

DWS-3160-24PC:admin#
```

To enable the RF scanning other channels and scanning interval time for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 rf_scan other_channel
mode enable
Command: config wireless ap_profile 1 radio 1 rf_scan other_channel mode enable

Success.

DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 rf_scan other_channel
interval 60
Command: config wireless ap_profile 1 radio 1 rf_scan other_channel interval 60

Success.

DWS-3160-24PC:admin#
```

To enable the RF sentry mode and scanning channels for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 rf_scan sentry mode
enable
Command: config wireless ap_profile 1 radio 1 rf_scan sentry mode enable

Success.

DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 rf_scan sentry
channels bgn
Command: config wireless ap_profile 1 radio 1 rf_scan sentry channels bgn

Success.

DWS-3160-24PC:admin#
```

To configure the RTS threshold for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 rts_threshold 2312
Command: config wireless ap_profile 1 radio 1 rts_threshold 2312

Success.

DWS-3160-24PC:admin#
```

To configure the Station Isolation mode for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 station_isolation
enable
Command: config wireless ap_profile 1 radio 1 station_isolation enable

Success.

DWS-3160-24PC:admin#
```

To enable VAP and settings associated with the network for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 vap 1 state enable
Command: config wireless ap_profile 1 radio 1 vap 1 state enable

Success.

DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 vap 1 network 2
Command: config wireless ap_profile 1 radio 1 vap 1 network 2

Success.

DWS-3160-24PC:admin#
```

To enable the WMM mode for the Radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#config wireless ap_profile 1 radio 1 wmm enable
Command: config wireless ap_profile 1 radio 1 wmm enable

Success.

DWS-3160-24PC:admin#
```

82-5 show wireless ap_profile

Description

This command is used to display the AP Profile configuration parameters. If no parameter is specified, a summary of the configured AP Profiles will be displayed. The detailed configuration includes radio, VAP, and QoS configuration.

Format

show wireless ap_profile {<int 1-16> {radio {<int 1-2> {[auto_eligible | mcs_index | qos {[ap_edca | station_edca]} | rates {[basic | supported]} | vap {<int 0-15>}]}}}}

Parameters

<int 1-16> - (Optional) Enter the configured AP profiles ID here. If you do not enter any command parameters, a summary of all AP profiles is displayed.

radio - (Optional) Specifies the radio configuration for an AP profile. When you enter the required profile ID, a summary view of the radio configuration is displayed. If you enter a radio index, the radio configuration detail is displayed.

<int 1-2> - Enter the radio configuration for an AP profile here. This value must be between 1 and 2.

auto_eligible - (Optional) Specifies to display supported channels on the radio that are eligible for auto-channel selection.

mcs_index - (Optional) Specifies to displays MCS information.

qos - (Optional) Specifies to display the configured values for a radio interface per QoS Queue (AP-EDCA and Station-EDCA).

ap_edca - Specifies to display the configured values for a radio interface per AP-EDCA QoS Queue.

station_edca - Specifies to display the configured values for a radio interface per Station-EDCA QoS Queue.

rates - (Optional) Specifies to display the list of supported and basic client data rates for the radio.

basic - Specifies to display the list of basic client data rates for the radio.

supported - Specifies to display the list of supported data rates for the radio.

vap - (Optional) Specifies that when you enter the required VAP ID, a summary view of the VAP configuration will be displayed. If you enter a VAP index, the VAP configuration detail is displayed.

<int 0-15> - Enter the required VAP ID value used here. This value must be between 0 and 15.

Restrictions

None.

Example

To display a summary of AP Profiles:

```
DWS-3160-24PC:admin#show wireless ap_profile
Command: show wireless ap_profile

AP Profile ID  Profile Name                      Profile Status
-------------  --------------------------------  -------------------
1              approfile                         Associated - Modified
2              Default                           Configured
3              Default                           Configured
4              Default                           Configured

Total Entries : 4

DWS-3160-24PC:admin#
```

To display a detailed configuration of AP Profile 1:

```
DWS-3160-24PC:admin#show wireless ap_profile 1
Command: show wireless ap_profile 1

AP Profile ID                                  : 1
Profile Name                                   : approfile
Hardware Type                                  : Any
Wired Network Detection VLAN ID                : 3
Disconnected AP Data Forwarding Mode           : Enable
Disconnected AP Management Mode                : Enable
Profile Status                                 : Associated - Modified
Valid APs Configured                           : 1
Managed APs Configured                         : 1

DWS-3160-24PC:admin#
```

To display a summary of AP Profile 1’s radios:

```
DWS-3160-24PC:admin#show wireless ap_profile 1 radio
Command: show wireless ap_profile 1 radio

AP Profile ID                                  : 1
Profile Name                                   : approfile
Radio Index  Status   Mode
-----------  -------  --------------------------------
1            On        802.11a/n
2            On        802.11b/g/n

DWS-3160-24PC:admin#
```

To display a detailed configuration of radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#show wireless ap_profile 1 radio 1
Command: show wireless ap_profile 1 radio 1

AP Profile ID                                  : 1
Profile Name                                   : approfile
```

```
Radio                                         : 1 - Sentry
Status                                        : On
Mode                                          : 802.11a/n
RF Scan - Other Channels Mode                 : Enable
RF Scan - Other Channels Scan Interval        : 60
RF Scan - Sentry Mode                         : Enable
RF Scan - Sentry Scan Channels                : 802.11b/g/n
RF Scan - Scan Duration                       : 2000
Enable Broadcast/Multicast Rate Limiting      : Enable
Broadcast/Multicast Rate Limit                : 20
Broadcast/Multicast Rate Limit Burst          : 30
Broadcast/Multicast Rate Limit Burst          : 30
DTIM Period                                   : 10
Fragmentation Threshold                       : 2312
RTS Threshold (bytes)                         : 2312
Short Retry Limit                             : 7
Long Retry Limit                              : 4
Maximum Transmit Lifetime                     : 512
Maximum Receive Lifetime                      : 512
Maximum Clients                               : 100
Automatic Channel Adjustment                  : Enable
Automatic Power Adjustment                    : Enable
Default Power (%)                             : 60
Load Balancing                                : Enable
Load Utilization (%)                          : 60
Station Isolation                             : Enable
Channel Bandwidth                             : 20 MHz
Primary Channel                               : Lower
Protection                                    : Auto
Short Guard Interval                          : Enabled
STBC Mode                                     : Enabled
Multicast Transmit Rate                       : 9 Mbps
UAPSD Mode                                    : Enable
No ACK                                        : Enable

DWS-3160-24PC:admin#
```

To display the auto-eligible lists of radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#show wireless ap_profile 1 radio 1 auto_eligible
Command: show wireless ap_profile 1 radio 1 auto_eligible

AP Profile ID                                 : 1
Profile Name                                  : approfile
Radio                                         : 1 - Sentry
Mode                                          : 802.11a/n

Supported Channels (* = Auto Eligible)        :
------------------------------------------------


   36*   40*   44*   48*  149*  153*  157*  161*
  165*



DWS-3160-24PC:admin#
```

To display the QoS configuration of radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#show wireless ap_profile 1 radio 1 qos
Command: show wireless ap_profile 1 radio 1 qos

AP Profile ID                                 : 1
Profile Name                                  : approfile
Radio                                         : 1 - Sentry
Mode                                          : 802.11a/n
Template                                      : Custom
WMM Mode                                      : Enable

AP EDCA Configuration
---------------------
QoS                        Minimum            Maximum        Maximum
Queues          AIFS   Contention Window  Contention Window   Burst
--------------  -----  -----------------  -----------------  --------
Voice (0)       1      3                  7                  1500
Video (1)       11     3                  7                  11
Best-Effort (2) 3      15                 63                 0
Background (3)  7      15                 1023               0

Station EDCA Configuration
-----------------------------
QoS                        Minimum            Maximum        Tx Op
Queues          AIFS   Contention Window  Contention Window  Limit
--------------  -----  -----------------  -----------------  --------
Voice (0)       22     7                  15                 222
Video (1)       2      7                  15                 94
Best-Effort (2) 3      15                 1023               0
Background (3)  7      15                 1023               0


DWS-3160-24PC:admin#
```

To display the basic rate lists and supported rate list of radio 1 of AP Profile 1:

```
DWS-3160-24PC:admin#show wireless ap_profile 1 radio 1 rates
Command: show wireless ap_profile 1 radio 1 rates

AP Profile ID                                 : 1
Profile Name                                  : approfile
Radio                                         : 1 - Sentry
Mode                                          : 802.11a/n

Advertised Rates (Mbps)
-----------------------
6 Mbps
9 Mbps
12 Mbps
24 Mbps

Supported Rates (Mbps)
-----------------------
6 Mbps
9 Mbps
12 Mbps
18 Mbps
24 Mbps
36 Mbps
48 Mbps
54 Mbps


DWS-3160-24PC:admin#
```

To display a summary of AP Profile radio 1’s VAPs:

```
DWS-3160-24PC:admin#show wireless ap_profile 1 radio 1 vap
Command: show wireless ap_profile 1 radio 1 vap

AP Profile ID                                 : 1
Radio                                         : 1

VAP  Mode      Network
---  --------  -----------------------------------
0    Enable    1 -dlink1
1    Enable    2 -dlink2
2    Disabled  3 -dlink3
3    Disabled  4 -dlink4
4    Disabled  5 -dlink5
5    Disabled  6 -dlink6
6    Disabled  7 -dlink7
7    Disabled  8 -dlink8
8    Disabled  9 -dlink9
9    Disabled  10-dlink10
10   Disabled  11-dlink11
11   Disabled  12-dlink12
12   Disabled  13-dlink13
13   Disabled  14-dlink14
14   Disabled  15-dlink15
15   Disabled  16-dlink16


DWS-3160-24PC:admin#
```

To display a detailed configuration of VAP 1 of AP Profile 1’s radio 1:

```
DWS-3160-24PC:admin#show wireless ap_profile 1 radio 1 vap 1
Command: show wireless ap_profile 1 radio 1 vap 1

AP Profile ID                                 : 1
Radio                                         : 1 - Sentry
Mode                                          : 802.11a/n
VAP ID                                        : 1
Mode                                          : Enable
Network                                       : 2-dlink2



DWS-3160-24PC:admin#
```

Chapter 83 Wireless AP Failure Status Command List

delete wireless ap_failed [<macaddr> | all]

delete wireless ap_failure list

show wireless ap_failure {<macaddr>}

83-1 delete wireless ap_failed

Description

This command is used to delete one or all managed AP entries with a failed status. A failed status indicates that the Wireless Switch has lost contact with the managed AP.

Format

delete wireless ap_failed [<macaddr> | all]

Parameters

<macaddr> - Enter the MAC address, of the falied managed AP, here.

all - Specifies that all failed managed AP entries, will be deleted.

Restrictions

Only Administrators can issue this command.

Example

To delete all managed AP entries with a failed status:

```
DWS-3160-24PC:admin#delete wireless ap_failed all
Command: delete wireless ap_failed all

Are you sure you want to delete all the failed managed AP entries? (y/n) y
delete wireless ap failed

All the failed managed AP entries deleted.

Success.

DWS-3160-24PC:admin#
```

83-2 delete wireless ap_failure list

Description

This command is used to delete all entries from the AP failure list. Entries will normally age out according to the configured age time. The AP failure list includes entries for all APs that have failed to validate or authenticate to the Wireless Switch.

Format

delete wireless ap_failure list

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To delete all entries from the AP failure list:

```
DWS-3160-24PC:admin#delete wireless ap_failure list
Command: delete wireless ap_failure list

Are you sure you want to clear the entire AP failure list? (y/n) y
clear wireless ap failure list

All AP failure entries cleared.

Success.

DWS-3160-24PC:admin#
```

83-3 show wireless ap_failure

Description

This command is used to display a summary or detailed information for entries in the AP failure list. Entries are added to the list when the Wireless Switch fails to validate or authenticate with an AP.

Format

show wireless ap_failure {<macaddr>}

Parameters

<macaddr> - (Optional) Enter the MAC address, of the failure AP, here.

Restrictions

None.

Example

To display summarized information of all failure APs:

```
DWS-3160-24PC:admin#show wireless ap_failure
Command: show wireless ap_failure

MAC Address
(*) Peer Managed   IP Address       Last Failure Type        Age
------------------ --------------- ------------------------ -------
 00-22-B0-3C-DD-C0  192.168.69.126 No Database Entry        0d:00:00:13

Total Entries : 1

DWS-3160-24PC:admin#
```

To displaying a specific failure AP status:

```
DWS-3160-24PC:admin#show wireless ap_failure 00-22-B0-3C-DD-C0
Command: show wireless ap_failure 00-22-B0-3C-DD-C0

MAC Address                        : 00-22-B0-3C-DD-C0
IP Address                         : 192.168.69.126
Reporting Switch                   : Local Switch
Switch MAC Address                 : 00-11-22-33-45-67
Switch IP Address                  : 192.168.69.123
Last Failure Type                  : No Database Entry
Validation Failure Count           : 1
Authentication Failure Count       : 1
Vendor ID                          : D-Link
Protocol Version                   : 2
Software Version                   : 4.0.0.1
Hardware Type                      : 9 - DWL-8600AP Dual Radio a/b/g/n
Age                                : 0d:00:00:07

DWS-3160-24PC:admin#
```

Chapter 84 Wireless Client Association Command List

config wireless client disassociate [all | <macaddr> | ap <macaddr> | ssid <ssid> | vap <macaddr>]
show wireless client {[summary | <macaddr> {[client_qos {radius} | neighbor ap | statistics {[association | session]} | dist_tunnel]}]}
show wireless ssid [<ssid> client | client]
show wireless switch client
show wireless vap {<macaddr>} client

84-1 config wireless client disassociate

Description

This command is used to initiate a request to disassociate a client, specified by the MAC address, or all clients associated to a WS managed AP, a particular SSID, or a particular VAP. The Wireless Switch sends a message to the appropriate managed AP to force the disassociation.

Format

config wireless client disassociate [all | <macaddr> | ap <macaddr> | ssid <ssid> | vap <macaddr>]

Parameters

all - Specifies to disassociate all clients associated.
<macaddr> - Enter an associated client MAC address, to disassociate, here.
ap - Specifies to disassociate all the clients, associated with the WS Managed AP. **<macaddr>** - Enter the MAC address of the WS Managed AP here.
ssid - Specifies to disassociate all the clients, associated with a particular SSID. **<ssid>** - Enter the SSID used here.
vap - Specifies to disassociate all the clients, associated with a particular VAP. **<macaddr>** - Enter the MAC address of the VAP here.

Restrictions

Only Administrators can issue this command.

Example

To disassociate all associated clients:

```
DWS-3160-24PC:admin#config wireless client disassociate all
Command: config wireless client disassociate all

Are you sure you want to disassociate all clients in the system? (y/n) y
Disassociate requested for all clients in the system.
Success.

DWS-3160-24PC:admin#
```

84-2 show wireless client

Description

This command is used to display a brief summary or detailed data for clients associated to a managed AP. If the Unified Switch is a Cluster Controller, this command will display all the associated clients in the peer-group. When acting as a Cluster Controller, the peer switch associated clients are displayed with an “*” (asterisk) before the Client MAC Address in the summary command.

Format

show wireless client {[summary | <macaddr> {[client_qos {radius} | neighbor ap | statistics {[association | session]} | dist_tunnel]}]}

Parameters

summary - (Optional) Specifies to display a brief summary of clients associated to a managed AP.

<macaddr> - (Optional) Enter the client MAC address used here.

client_qos - (Optional) Specifies to display detailed client QoS data for the client.
radius - Specifies to display the configured values successfully obtained from a RADIUS server for the specified client.

neighbor ap - (Optional) Specifies to display all the APs that an associated client can see in its RF area.

statistics - (Optional) Specifies to display statistics for a specified client.
association - Specifies to display association statistics for a specified client.
session - Specifies to display session statistics for a specified client.

dist_tunnel - Specifies that Layer 2 distributed tunnel information will be displayed.

Restrictions

None.

Example

To display the client summary:

```
DWS-3160-24PC:admin#show wireless client summary
Command: show wireless client summary

    MAC Address
(*) Peer Managed   IP Address        NetBIOS Name
------------------ ----------------- -----------------
*00-15-E9-C3-EB-77 192.168.69.69     W0ND3RB0-EM4D20

Total Entries : 1

DWS-3160-24PC:admin#
```

To displaying the QoS of a specified client:

```
DWS-3160-24PC:admin#show wireless client 00-15-E9-C3-EB-77 client_qos
Command: show wireless client 00-15-E9-C3-EB-77 client_qos

MAC address                                   : 00-15-E9-C3-EB-77
SSID                                          : DWS01
Client QoS Operational Status                 : Disabled
Bandwidth Limit Down                          : 0
Bandwidth Limit Up                            : 0
Access Control Down                           : <none>
Access Control Up                             : <none>
Diffserv Policy Down                          : <none>
Diffserv Policy Up                            : <none>

DWS-3160-24PC:admin#
```

To display the QoS RADIUS information of a specified client:

```
DWS-3160-24PC:admin#show wireless client 00-15-E9-C3-EB-77 client_qos radius
Command: show wireless client 00-15-E9-C3-EB-77 client_qos radius

MAC address                                   : 00-15-E9-C3-EB-77
SSID                                          : DWS01
Bandwidth Limit Down                          : <none>
Bandwidth Limit Up                            : <none>
Access Control Down                           : <none>
Access Control Up                             : <none>
Diffserv Policy Down                          : <none>
Diffserv Policy Up                            : <none>

DWS-3160-24PC:admin#
```

To display the neighbor AP of the specified client:

```
DWS-3160-24PC:admin#show wireless client 00-15-E9-C3-EB-77 neighbor ap
Command: show wireless client 00-15-E9-C3-EB-77 neighbor ap

AP MAC Address    Location               Radio Discovery Reason
----------------- ---------------------- ----- --------------------------------
00-22-B0-3C-43-C0                        1     Assoc this AP,RF
00-22-B0-3C-43-C0                        2     RF
00-22-B0-3C-DD-C0                        1     Assoc Managed AP,RF
00-22-B0-3C-DD-C0                        2     Assoc Managed AP,RF

Total Entries : 4

DWS-3160-24PC:admin#
```

To display statistics of a specified client:

```
DWS-3160-24PC:admin#show wireless client 00-15-E9-C3-EB-77 statistics
Command: show wireless client 00-15-E9-C3-EB-77 statistics

MAC address                                 : 00-15-E9-C3-EB-77
Packets Received                            : 210
Packets Transmitted                         : 198
Bytes Received                              : 37472
Bytes Transmitted                           : 105559
Packets Receive Dropped                     : 0
Packets Transmit Dropped                    : 0
Bytes Receive Dropped                       : 0
Bytes Transmit Dropped                      : 0
Duplicate Packets Received                  : 245
Packet Fragments Received                   : 0
Packet Fragments Transmitted                : 0
Transmit Retry Count                        : 40
Failed Retry Count                          : 1

DWS-3160-24PC:admin#
```

To display association statistics of a specified client:

```
DWS-3160-24PC:admin#show wireless client 00-15-E9-C3-EB-77 statistics
association
Command: show wireless client 00-15-E9-C3-EB-77 statistics association

MAC address                                 : 00-15-E9-C3-EB-77
Packets Received                            : 210
Packets Transmitted                         : 198
Bytes Received                              : 37472
Bytes Transmitted                           : 105559
Packets Receive Dropped                     : 0
Packets Transmit Dropped                    : 0
Bytes Receive Dropped                       : 0
Bytes Transmit Dropped                      : 0
Duplicate Packets Received                  : 245
Packet Fragments Received                   : 0
Packet Fragments Transmitted                : 0
Transmit Retry Count                        : 40
Failed Retry Count                          : 1

DWS-3160-24PC:admin#
```

To display session statistics of a specified client:

```
DWS-3160-24PC:admin#show wireless client 00-15-E9-C3-EB-77 statistics session
Command: show wireless client 00-15-E9-C3-EB-77 statistics session

MAC address                                  : 00-15-E9-C3-EB-77
Packets Received                             : 220
Packets Transmitted                          : 207
Bytes Received                               : 38591
Bytes Transmitted                            : 110541
Packets Receive Dropped                      : 0
Packets Transmit Dropped                     : 0
Bytes Receive Dropped                        : 0
Bytes Transmit Dropped                       : 0
Duplicate Packets Received                   : 285
Packet Fragments Received                    : 0
Packet Fragments Transmitted                 : 0
Transmit Retry Count                         : 40
Failed Retry Count                           : 1

DWS-3160-24PC:admin#
```

In the above examples the following display parameters can be noticed:

MAC Address - Displays the Ethernet address of the client station.

VAP MAC Address - Displays the Ethernet MAC address for the managed AP VAP where this client is associated.

SSID - Displays the network on which the client is connected.

Status - Displays whether or not the client has associated and/or authenticated. The valid values are:

- **Associated** - The client is currently associated to the managed AP.
- **Authenticated** - The client is currently associated and authenticated to the managed AP.
- **Disassociated** - The client has disassociated from the managed AP. If the client does not roam to another managed AP within the client roam timeout, it will be deleted.

Network Time - Displays the time since the client first authenticated with the network.

IP Address - Displays the network IP address of client.

NetBIOS Name - Displays the NETBIOS name of the client.

Client QoS Operational Status - Displays whether client QoS operation is enabled on this network.

Bandwidth Limit Down - Displays the default maximum rate limit in bits per second for traffic flowing from the AP to the client. A value of 0 disables rate limiting in this direction. This default is used for clients that do not obtain their own value via RADIUS.

Bandwidth Limit Up - Displays the default maximum rate limit in bits per second for traffic flowing from the client to the AP. A value of 0 disables rate limiting in this direction. This default is used for clients that do not obtain their own value via RADIUS.

Access Control Down - Displays the default access control list to use for traffic flowing from the AP to the client. Both the ACL type and its name (or number) is displayed. This default is used for clients that do not obtain their own value via RADIUS.

Access Control Up - Displays the default access control list to use for traffic flowing from the client to the AP. Both the ACL type and its name (or number) is displayed. This default is used for clients that do not obtain their own value via RADIUS.

Diffserv Policy Down - Displays the default Diffserv policy to use for traffic flowing from the AP to the client. This default is used for clients that do not obtain their own value via RADIUS.

Diffserv Policy Up - Displays the default Diffserv policy to use for traffic flowing from the client to the AP. This default is used for clients that do not obtain their own value via RADIUS.

AP MAC Address - Displays the base Ethernet address of the WS managed AP.

Location - Displays the configured descriptive location for the managed AP

Radio - Displays the radio on the managed AP that detected this client as a neighbor.

Discovery Reason - Displays one or more discovery methods for the neighbor client. One or more of the following abbreviated values may be displayed:

- **RF Scan (RF)** - The client was reported from an RF scan on the radio. Note that client stations are difficult to detect via RF scan, the other methods are more common for client neighbor detection.
- **Probe Request (Probe)** - The managed AP received a probe request from the client.
- **Associated to Managed AP (Assoc Managed AP)** - This neighbor client is associated to another managed AP.
- **Associated to this AP (Assoc this AP)** - The client is associated to this managed AP on the displayed radio.
- **Associated to Peer AP (Assoc peer AP)** - The client is associated to a peer switch managed AP.
- **Ad Hoc Rogue (Ad Hoc)** - The client was detected as part of an ad hoc network.

Packets Received - Displays the total packets received from the client station.

Packets Transmitted - Displays the total packets transmitted to the client station.

Bytes Received - Displays the total bytes received from the client station.

Bytes Transmitted - Displays the total bytes transmitted to the client station.

Packets Receive Dropped - Displays the total receive packets from the client station that were discarded by the AP.

Packets Transmit Dropped - Displays the totals packets discarded by the AP prior to transmission to the client station.

Bytes Receive Dropped - Displays the total receive bytes from the client station that were discarded by the AP.

Bytes Transmit Dropped - Displays the total bytes discarded by the AP prior to transmission to the client station.

Duplicate Packets Received - Displays the total duplicate packets received from the client station.

Packet Fragments Received - Displays the total fragmented packets received from the client station.

Packet Fragments Transmitted - Displays the total fragmented packets transmitted to the client station.

Transmit Retry Count - Displays the number of times transmits to the client station succeeded after one or more retries.

Failed Retry Count - Displays the number of times transmits to the client station failed after one or more retries.

Detected IP Address - Displays the IPv4 address detected for the clients using ARP snooping.

Switch MAC Address - Displays the Ethernet address of the WS associating this client.

Switch IP Address - Displays the network IP address of the WS associating this client.

Tunnel IP Address - Displays ‘---‘ field for all non-tunneled clients. For a tunneled client, this is the assigned tunnel IP address.

To display Layer 2 distributed tunnel information of an associated client:

```
DWS-3160-24PC:admin#show wireless client 00-15-E9-C3-EB-77 dist_tunnel
Command: show wireless client 00-15-E9-C3-EB-77 dist_tunnel

 MAC address                                  : 00-15-E9-C3-EB-77
 VAP MAC Address                              : 00-22-B0-3C-43-C0
 AP MAC Address                               : 00-22-B0-3C-43-C0
 Associating Switch                           : Peer Switch
 Switch MAC Address                           : 00-11-22-33-32-32
 Switch IP Address                            : 192.168.69.124
 Distributed Tunneling Status                 : Disabled
 Distributed Tunnel Client Roam Status        : ------
 Distributed Tunnel Home AP MAC Address       : ------
 Distributed Tunnel Associated AP MAC Address : ------


DWS-3160-24PC:admin#
```

In the above example the following display parameters can be noticed:

MAC address - Displays the client’s MAC address.

VAP MAC Address - Displays the connected VAP’s MAC address.

AP MAC Address - Displays the conneected AP’s MAC address.

Associating Switch - Displays the associating Switch type. The two display options are “**Peer Switch**" or "**Local Switch**”.

Switch MAC Address - Displays the MAC address of associating Switch.

Switch IP Address - Displays the IP address of associating Switch.

Distributed Tunneling Status - Displays whether this client is associated with a network that supports Layer 2 distributed tunneling or not.

Distributed Tunnel Client Roam Status - Displays whether the client is on the Home AP or has roamed to another AP and is using a tunnel.
The field can display one of the following values:
Home - Specifies that the client is not using a tunnel.
Roaming - Specifies that the client is using a tunnel.
If distributed tunneling is disabled, the field displays the roam status as ‘------‘.

Distributed Tunnel Home AP MAC Address - Displays the MAC Address of the Home AP for the client. The value is meaningful only for clients that are associated with networks enabled for distributed tunneling.

Distributed Tunnel Associated AP MAC Address - Displays the MAC Address of the AP to which the client roamed via the distributed tunneling protocol.

84-3 show wireless ssid

Description

This command is used to display summary data for all managed SSIDs with associated clients. If the optional SSID string is specified, the display will only show clients associated to that network. An SSID/network may exist on one or more managed AP VAPs.

Format

show wireless ssid [<ssid> client | client]

Parameters

<ssid> - Enter the Service Set Identifier (SSID), for the network, here.

client - Specifies that client stations will be displayed.
client - Specifies that client stations will be displayed.

Restrictions

None.

Example

To display associated clients on all managed SSIDs:

```
DWS-3160-24PC:admin#show wireless ssid client
Command: show wireless ssid client

                                       Client
             SSID                   MAC Address
------------------------------- -----------------
DWS01                            00-15-E9-C3-EB-77

Total Entries : 1

DWS-3160-24PC:admin#
```

To display associated clients on a specific SSID:

```
DWS-3160-24PC:admin#show wireless ssid "DWS01" client
Command: show wireless ssid "DWS01" client

                                       Client
             SSID                   MAC Address
------------------------------- -----------------
DWS01                            00-15-E9-C3-EB-77

Total Entries : 1

DWS-3160-24PC:admin#
```

84-4 show wireless switch client

Description

This command is used to display summary data for all Switches with associated clients. If the Wireless Switch is a Cluster Controller, then this command shows all clients associated to the APs, managed by all the peer Switches. For non-Cluster Controller Switches, only clients, managed by the local Switches, are displayed.

Format

show wireless switch client

Parameters

None.

Restrictions

None.

Example

To display summary data for all Switches with associated clients:

```
DWS-3160-24PC:admin#show wireless switch client
Command: show wireless switch client

Switch IP Address  Client MAC Address
-----------------  ------------------
192.168.69.124     00-15-E9-C3-EB-77

Total Entries : 1

DWS-3160-24PC:admin#
```

84-5 show wireless vap

Description

This command is used to display summary data for all managed AP VAPs with associated clients. If the optional VAP MAC address is specified, the display will only show clients associated to the specific managed AP VAP.

Format

show wireless vap {<macaddr>} client

Parameters

<macaddr> - (Optional) Enter the WS managed AP VAP MAC address here.
client - Specifies to display summary data for managed AP VAPs with associated clients.

Restrictions

None.

Example

To display summary data for all managed AP VAPs with associated clients:

```
DWS-3160-24PC:admin#show wireless vap client
Command: show wireless vap client

 VAP MAC Address   AP MAC Address        Location      Radio Client MAC Address
----------------- ----------------- ------------------ ----- ------------------
00-22-B0-3C-43-C0 00-22-B0-3C-43-C0                    1     00-15-E9-C3-EB-77

Total Entries : 1

DWS-3160-24PC:admin#
```

To display clients associated to the specific managed AP VAP:

```
DWS-3160-24PC:admin#show wireless vap 00-22-B0-3C-43-C0 client
Command: show wireless vap 00-22-B0-3C-43-C0 client

 VAP MAC Address   AP MAC Address        Location      Radio Client MAC Address
----------------- ----------------- ------------------ ----- ------------------
00-22-B0-3C-43-C0 00-22-B0-3C-43-C0                    1     00-15-E9-C3-EB-77

Total Entries : 1

DWS-3160-24PC:admin#
```

Chapter 85 Wireless Ad Hoc Status Command List

delete wireless adhoc_list
show wireless adhoc {<macaddr>}

85-1 delete wireless adhoc_list

Description

This command is used to delete all entries from the Ad Hoc client list. Entries normally age out according to the configured age time.

Format

delete wireless adhoc_list

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To delete all entries from the Ad Hoc client list:

```
DWS-3160-24PC:admin#delete wireless adhoc_list
Command: delete wireless adhoc_list

Are you sure you want to delete all Ad Hoc client entries? (y/n) y
All Ad Hoc client entries deleted.
Success.

DWS-3160-24PC:admin#
```

85-2 show wireless adhoc

Description

This command is used to display summary or detailed data for Ad Hoc clients detected on the network by a managed AP.

Format

show wireless adhoc {<macaddr>}

Parameters

<macaddr> - (Optional) Enter the client MAC address here.

Restrictions

None.

Example

To display a summary of the Ad Hoc list:

```
DWS-3160-24PC:admin# show wireless adhoc
Command: show wireless adhoc

MAC Address       AP MAC Address    Location   Radio Det. Mode Age
----------------- ----------------- ---------- ----- --------- ----------------
00-01-01-30-01-01 00-01-01-02-01-01 FirstFloor 1     Beacon    0d:00:06:31
00-01-01-42-01-01 00-01-01-02-03-01 Eng        1     Beacon    0d:00:06:34
00-01-01-45-01-01 00-01-01-02-01-01 FirstFloor 1     Beacon    0d:00:06:36

Total Entries : 3

DWS-3160-24PC:admin#
```

Chapter 86 Wireless Detected Client Database Command List

delete wireless detected_client [all | <macaddr>]
config wireless detected_client ack_rogue [all | <macaddr>]
config wireless detected_client preauth_history_purge [all | <macaddr>]
config wireless detected_client roam_history_purge [all | <macaddr>]
show wireless detected_client {<macaddr>}
show wireless detected_client pre_auth_history {<macaddr>}
show wireless detected_client roam_history {<macaddr>}
show wireless detected_client rogue_classification <macaddr>
show wireless detected_client triangulation <macaddr>

86-1 delete wireless detected_client

Description

This command is used to delete the client entry for the specified MAC address or all the entries present in the database. If the client has authenticated, then this command has no effect.

Format

delete wireless detected_client [all | <macaddr>]

Parameters

all - Specifies that all entries, present in detected-client database, will be deleted.
<macaddr> - Enter the MAC address of the specified client here.

Restrictions

Only Administrators can issue this command.

Example

To delete all the entries present in the database:

```
DWS-3160-24PC:admin#delete wireless detected_client all
Command: delete wireless detected_client all

Are you sure you want to clear the entire detected client list? (y/n) y
All detected client entries cleared.
Success.

DWS-3160-24PC:admin#
```

86-2 config wireless detected_client ack_rogue

Description

This command is used to change the detected client’s status from rogue to known or authenticated.

Format

config wireless detected_client ack_rogue [all | <macaddr>]

Parameters

ack_rogue - Specifies to change the client status from Rogue to Known or Authenticated for the specified client MAC address or all the clients present in the detected client database.

all - Specifies to change all the clients present in the detected client database.

<macaddr> - Enter the MAC address of a specific client here.

Restrictions

Only Administrators can issue this command.

Example

To acknowledge all rogue clients:

```
DWS-3160-24PC:admin#config wireless detected_client ack_rogue all
Command: config wireless detected_client ack_rogue all

Are you sure you want to acknowledge all rogue client status
in the Detected clients database? (y/n) y
All rogue clients acknowledged.
Success.

DWS-3160-24PC:admin#
```

86-3 config wireless detected_client preauth_history_purge

Description

This command is used to clear the detected client’s pre-authentication history.

Format

config wireless detected_client preauth_history_purge [all | <macaddr>]

Parameters

preauth_history_purge - Specifies to clear the pre-authentication history maintained for the specified MAC address or all the clients present in the detected client database.

all - Specifies to clear the pre-authentication history maintained for all the clients present in the detected client database.

<macaddr> - Enter the MAC address of a specific client here.

Restrictions

Only Administrators can issue this command.

Example

To clear the pre-authentication history maintained for all the clients present in the detected client database:

```
DWS-3160-24PC:admin#config wireless detected_client preauth_history_purge all
Command: config wireless detected_client preauth_history_purge all

Are you sure you want to clear the pre-auth-history for all the detected
clients? (y/n) y
Preauth history cleared for all the detected clients.
Success.

DWS-3160-24PC:admin#
```

86-4 config wireless detected_client roam_history_purge

Description

This command is used to clear the detected client's roaming history.

Format

config wireless detected_client roam_history_purge [all | <macaddr>]

Parameters

roam_history_purge - Specifies to clear the roaming history maintained for a specific MAC address or all the clients present in the detected client database.

all - Specifies to clear the roaming history maintained for all the clients present in the detected client database.

<macaddr> - Enter the MAC address of a specific client here.

Restrictions

Only Administrators can issue this command.

Example

To clear the roaming history maintained for all the clients present in the detected client database:

```
DWS-3160-24PC:admin#config wireless detected_client roam_history_purge all
Command: config wireless detected_client roam_history_purge all

Are you sure you want to clear the roam-history for all the detected
clients? (y/n) y
Roam history cleared for all the detected clients.
Success.

DWS-3160-24PC:admin#
```

86-5 show wireless detected_client

Description

This command is used to display the status of the detected clients.

Format

show wireless detected_client {<macaddr>}

Parameters

<macaddr> - (Optional) Enter the MAC address of the specified detected client here.

Restrictions

None.

Example

To display the status information for all the detected clients:

```
DWS-3160-24PC:admin# show wireless detected_client
Command: show wireless detected_client

MAC Address       Client Name     Client Status  Age           Create Time
----------------- --------------- -------------- ------------- -------------
00-17-9A-D1-66-A5                 Detected       0d:00:10:01   0d:00:12:02
00-1D-6A-12-0F-C1                 Detected       0d:00:10:31   0d:00:12:02
00-25-D3-99-49-4D                 Detected       0d:00:10:31   0d:00:11:31
5C-33-8E-0D-18-63                 Detected       0d:00:12:02   0d:00:12:02
68-A3-C4-CA-CC-8D                 Detected       0d:00:10:31   0d:00:11:31
70-F3-95-3A-05-CC                 Detected       0d:00:11:02   0d:00:12:02
F4-9F-54-6B-48-50                 Detected       0d:00:11:02   0d:00:11:31

Total Entries : 7

DWS-3160-24PC:admin#
```

86-6 show wireless detected_client pre_auth_history

Description

This command is used to display the pre-authentication history of the detected clients.

Format

show wireless detected_client pre_auth_history {<macaddr>}

Parameters

pre_auth_history - Specifies the pre-authentication events that have occurred for clients in the detected client database. A history of up to ten pre-authentications is displayed, as only a maximum of ten pre-authentications are maintained for each client

<macaddr> - (Optional) Enter the MAC address of the specified detected client here.

Restrictions

None.

Example

To display all detected clients' pre-authentication history:

```
DWS-3160-24PC:admin# show wireless detected_client pre_auth_history
Command: show wireless detected_client pre_auth_history

MAC Address       AP MAC Address
----------------- ------------------------------------------------------------
00-02-BB-00-0A-02 <-00-22-BB-00-14-00 <-00-00-91-00-50-00 <-00-22-BB-00-14-00
                  <-00-00-91-00-50-00
00-02-BB-00-0A-03 <-00-22-BB-00-14-00
00-02-BB-00-0A-04 <-00-22-BB-00-14-00 <-00-00-91-00-50-00 <-00-22-BB-00-14-00
                  <-00-00-91-00-50-00 <-00-00-87-00-50-10 <-00-22-BB-00-14-00
                  <-00-00-91-00-50-00 <-00-00-87-00-50-10 <-00-22-BB-00-14-00
                  <-00-00-91-00-50-00

Total History Entries : 15

DWS-3160-24PC:admin#
```

To display the pre-authentication history of a specific client detected:

```
DWS-3160-24PC:admin# show wireless detected_client pre_auth_history
00:02:BB:00:0A:01
Command: show wireless detected_client pre_auth_history 00-02-BB-00-0A-01

AP MAC Addr(Radio)   VAP MAC Address   SSID                Pre-Auth Time Since
                                                           Status   Event
-------------------- ----------------- ------------------- -------- ----------
00-22-BB-00-0A-00(1) 00-22-BB-00-0A-01 Test Network1       Success  0d:00:01:51
00-22-BB-00-14-10(2) 00-22-BB-00-14-12 Test Network3       Failure  0d:00:04:40
00-22-BB-00-0A-00(1) 00-22-BB-00-0A-01 Test Network2       Success  0d:00:04:51
00-22-BB-00-14-10(2) 00-22-BB-00-14-13 Network3            Failure  0d:00:05:40
00-02-BB-00-0A-00(1) 00-02-BB-00-0A-01 Test Network3       Success  0d:00:11:51
00-00-91-00-50-10(2) 00-00-91-00-50-12 Test Network1       Failure  0d:00:14:40
00-00-87-00-50-00(1) 00-00-87-00-50-08 Test Network1       Success  0d:00:14:51
00-00-92-00-50-00(1) 00-00-92-00-50-02 Broadcom Network    Failure  0d:00:15:40

DWS-3160-24PC:admin#
```

86-7 show wireless detected_client roam_history

Description

This command is used to display the roaming history of the detected clients.

Format

show wireless detected_client roam_history {<macaddr>}

Parameters

roam_history - Specifies the roaming history for the clients in the detected client database. A roaming history of up to ten Access Points is displayed, as only a maximum of ten records are maintained for each client. Clients that never authenticated with the managed network are not displayed in this list.

<macaddr> - (Optional) Enter the MAC address of the specified detected client here.

Restrictions

None.

Example

To display all the detected clients' roam history:

```
DWS-3160-24PC:admin# show wireless detected_client roam_history
Command: show wireless detected_client roam_history

Mac Address       AP MAC Address
----------------- ---------------------------------------------------------
00-02-BB-00-0A-01 <-00-22-BB-00-14-00 <-00-00-91-00-50-00 <-00-22-BB-00-14-00
                  <-00-00-91-00-50-00 <-00-00-87-00-50-10 <-00-22-BB-00-14-00
                  <-00-00-91-00-50-00 <-00-00-87-00-50-10 <-00-22-BB-00-14-00
                  <-00-00-91-00-50-00
00-02-BB-00-0A-02 <-00-22-BB-00-14-00 <-00-00-91-00-50-00 <-00-22-BB-00-14-00
                  <-00-00-91-00-50-00
00-02-BB-00-0A-03 <-00-22-BB-00-14-00

Total History Entries : 15

DWS-3160-24PC:admin#
```

To display the roam history of a specific client detected:

```
DWS-3160-24PC:admin# show wireless detected_client roam_history
00:02:BB:00:0A:01
Command: show wireless detected_client roam_history 00-02-BB-00-0A-01

AP MAC Addr(Radio)   VAP MAC Address    SSID              Auth      Time Since
                                                          Status    Event
-------------------- ----------------- ----------------- -------- ----------
00-02-BB-00-0A-00(1) 00-02-BB-00-0A-07 Network8          Roam      0d:00:01:51
00-02-BB-00-0A-00(1) 00-02-BB-00-0A-01 TestNetwork2      New Auth  0d:00:02:40
00-02-92-00-0A-10(2) 00-02-92-00-0A-10 Network1          New Auth  0d:00:02:51
00-02-92-00-0A-10(2) 00-02-92-00-0A-12 TestNetwork3      Roam      0d:00:14:40

DWS-3160-24PC:admin#
```

86-8 show wireless detected_client rogue_classification

Description

This command is used to display the WIDS rogue classification test results for a particular client MAC address.

Format

show wireless detected_client rogue_classification <macaddr>

Parameters

rogue_classification - Specifies the WIDS rogue classification test results for a particular client MAC address.	
<macaddr> - Enter the MAC address of the specified detected client here.	

Restrictions

None.

Example

To display the detected client rogue-classification:

```
DWS-3160-24PC:admin#show wireless detected_client rogue_classification F4-9F-
54-6B-48-50
Command: show wireless detected_client rogue_classification F4-9F-54-6B-48-50

               Cond                          Test    Test   Time Since Time Since
Test ID        Detect MAC Addr (radio)       Config  Result 1st Report Last Report
-------------- ----- -------------------- ------- ----- ----------- -----------
WIDSCLNTROGUE1 True  00-22-B0-3C-43-C0(2) Disable       0d:00:17:39 0d:00:17:10
WIDSCLNTROGUE2 False 00-22-B0-3C-43-C0(2) Enable        0d:00:37:59 0d:00:17:10
WIDSCLNTROGUE3 False 00-22-B0-3C-43-C0(2) Enable        0d:00:37:59 0d:00:17:10
WIDSCLNTROGUE4 False 00-22-B0-3C-43-C0(2) Enable        0d:00:37:59 0d:00:17:10
WIDSCLNTROGUE5 False 00-22-B0-3C-43-C0(2) Enable        0d:00:37:59 0d:00:17:10
WIDSCLNTROGUE6 False 00-22-B0-3C-43-C0(2) Disable       0d:00:37:59 0d:00:17:10
WIDSCLNTROGUE7 True  00-22-B0-3C-43-C0(2) Disable       0d:00:17:39 0d:00:17:10

WIDSCLNTROGUE1        : Known Client Database Test
WIDSCLNTROGUE2        : Client exceeds configured rate for auth msgs
WIDSCLNTROGUE3        : Client exceeds configured rate for probe msgs
WIDSCLNTROGUE4        : Client exceeds configured rate for de-auth msgs
WIDSCLNTROGUE5        : Client exceeds max failing authentications
WIDSCLNTROGUE6        : Known client authenticated with unknown AP
WIDSCLNTROGUE7        : Client OUI not in the OUI Database

DWS-3160-24PC:admin#
```

86-9 show wireless detected_client triangulation

Description

This command is used to display the signal triangulation status for the specified client entry.

Format

show wireless detected_client triangulation <macaddr>

Parameters

triangulation - Specifies the signal triangulation status for the specified client entry.

<macaddr> - Enter the MAC address of the specified detected client here.

Restrictions

None.

Example

To display the signal triangulation status for the specified client entry:

```
DWS-3160-24PC:admin#show wireless detected_client triangulation F4-9F-54-6B-48-
50
Command: show wireless detected_client triangulation F4-9F-54-6B-48-50


                                     RSSI Signal Noise
AP Function AP MAC Address    Radio   (%)  (dBm) (dBm) Age
----------- ----------------- ----- ----- ------ ----- -----------
 Non-Sentry 00-22-B0-3C-43-C0     2     1    -90   -92 0d:00:17:41

DWS-3160-24PC:admin#
```

Chapter 87 Wireless Local Access Point Database Command List

create wireless ap_database <macaddr>

delete wireless ap_database [<macaddr> | all]

config wireless ap_database <macaddr> [location [<desc 1-32> | clear] | mode [ws_managed [profile [<int 1-16> | default] | password {encrypted <password 128>} | radio <int 1-2> {channel <int 0-165> | power <int 0-100>}] | standalone [channel [<int 0-165> | default] | security [any | open | wep | wpa | default] | ssid [<desc 1-32> | clear] | wire_mode [allowed | not_allowed | default]] | rogue]]

show wireless ap_database {<macaddr>}

87-1 create wireless ap_database

Description

This command is used to add an AP to the local valid AP database.

Format

create wireless ap_database <macaddr>

Parameters

<macaddr> - Enter the MAC address of a physical AP here.

Restrictions

Only Administrators can issue this command.

Example

To add an AP to the local valid AP database:

```
DWS-3160-24PC:admin#create wireless ap_database 00-22-B0-3D-AB-40
Command: create wireless ap_database 00-22-B0-3D-AB-40

Success.

DWS-3160-24PC:admin#
```

87-2 delete wireless ap_database

Description

This command is used to delete an AP entry, using the specified MAC address, from the local database or all the entries present from the database.

Format

delete wireless ap_database [<macaddr> | all]

Parameters

<macaddr> - Enter the MAC address of a physical AP here.

all - Specifies that all AP entries, present in local AP database, will be deleted.

Restrictions

Only Administrators can issue this command.

Example

To delete all AP entries:

```
DWS-3160-24PC:admin#delete wireless ap_database all
Command: delete wireless ap_database all

Success.

DWS-3160-24PC:admin#
```

87-3 config wireless ap_database

Description

This command is used to configure the AP settings identified by the AP MAC address. In this command, the user can configure parameters for each individual valid AP.

NOTE: If a valid AP is already being managed by the Switch, the user needs to reboot the AP to pick up any configuration changes in the valid AP database.

Format

config wireless ap_database <macaddr> [location [<desc 1-32> | clear] | mode [ws_managed [profile [<int 1-16> | default] | password {encrypted <password 128>} | radio <int 1-2> {channel <int 0-165> | power <int 0-100>}] | standalone [channel [<int 0-165> | default] | security [any | open | wep | wpa | default] | ssid [<desc 1-32> | clear] | wire_mode [allowed | not_allowed | default]] | rogue]]

Parameters

<macaddr> - Enter the MAC address of a physical AP here.

location - Specifies a descriptive string for the AP location.

<desc 1-32> - Enter the AP location name used here. This name can be up to 32 characters long.

clear - Specifies that the descriptive string for the AP location will be cleared.

mode - Specifies the managed mode for an AP.

ws_managed - Specifies that AP will be managed by the Wireless Switch upon discovery. This is the default managed mode.

profile - Specifies the AP profile ID for AP configuration.

<int 1-16> - Enter the AP profile ID value used here. This value must be between 1 and

16. The default option is 1.

default - Specifies that the default value will be used.

password - Specifies the password that AP must used to authenticate to the Wireless Switch. The password is only verified if global AP authentication is enabled. After entering the password, the CLI will prompt the user to enter a password that is between 8-63 alphanumeric characters long.

encrypted - (Optional) Specifies that the password will be encrypted.

<password 128> - Enter the password, used for AP authentication to this Switch, here. This value can be up to 128 alphanumeric characters long.

radio - Specifies the radio interface on the AP.

<int 1-2> - Enter the radio interface value used here. This value must be either 1 or 2.

channel - (Optional) Specifies the wireless channel number for the radio. The valid range is based on the configured country code.

<int 0-165> - Enter the wireless channel number, used on the AP, here. This value must be between 0 and 165. The value 0 means that the channel will be assigned automatically.

power - (Optional) Specifies the transmit power value for the radio. The value is entered is the percentage of the maximum power.

<int 0-100> - Enter the transmit power value, used for the radio, here. This value must be between 0 and 100 percent. The unit used is %. The value ‘0’ means that the transmit power will be calculated automatically.

standalone - Specifies that the AP is managed as a standalone AP and should not be reported as rogue by the Wireless Switch.

channel - Specifies the wireless channel number for the radio. The valid range is based on the configured country code.

<int 0-165> - Enter a valid channel from the 'all-country' aggregate channel list here. This value must be between 0 and 165. Channel '0' indicates that any valid channel is allowed. The default value is 0.

default - Specifies that the default value will be used.

security - Specifies the expected security mode for an AP in stand-alone mode.

any - Specifies that all security modes are allowed. Security modes available are open security, WEP and WPA/WPA2. This is the default option.

open - Specifies that only the open security mode is allowed for the AP.

wep - Specifies that only the WEP security mode is allowed for the AP.

wpa - Specifies that only WPA or WPA2 security modes are allowed for the AP.

default - Specifies that the default option will be used.

ssid - Specifies the expected SSID for an AP in stand-alone mode. Default: “” (empty **string** – any SSID is allowed).

<desc 1-32> - Enter the expected SSID for an AP in stand-alone mode here. This string can be up to 32 characters long.

clear - Specifies to clear the expected SSID for an AP in stand-alone mode.

wire_mode - Specifies that expected wired mode, for an AP in stand-alone mode, will be used.

allowed - Specifies that the AP is allowed to be on the wired network. This is the default option.

not_allowed - Specifies that the AP is not allowed on the wired network.

default - Specifies that the default option will be used.

rogue - Specifies that the AP is identified as an administrator, configured rogue AP, and will be reported as rogue upon discovery.

Restrictions

Only Administrators can issue this command.

Example

To configure the AP location:

```
DWS-3160-24PC:admin#config wireless ap_database 00-22-B0-3C-DD-C0 location 5F
Command: config wireless ap_database 00-22-B0-3C-DD-C0 location 5F

Success.

DWS-3160-24PC:admin#
```

To configure the AP in managed mode and using profile 1:

```
DWS-3160-24PC:admin#config wireless ap_database 00-22-B0-3C-DD-C0 mode
ws_managed profile 1
Command: config wireless ap_database 00-22-B0-3C-DD-C0 mode ws_managed profile
1

Success.

DWS-3160-24PC:admin#
```

To configure the managed AP to use channel 36:

```
DWS-3160-24PC:admin#config wireless ap_database 00-22-B0-3C-DD-C0 mode
ws_managed radio 1 channel 36
Command: config wireless ap_database 00-22-B0-3C-DD-C0 mode ws_managed radio 1
channel 36

Success.

DWS-3160-24PC:admin#
```

To configure the stand-alone AP to use an SSID of “123”:

```
DWS-3160-24PC:admin#config wireless ap_database 00-22-B0-3C-DD-C0 mode
standalone ssid 123
Command: config wireless ap_database 00-22-B0-3C-DD-C0 mode standalone ssid 123

 AP mode has been changed. The change will not take effect until the AP is
reboot.

Success.

DWS-3160-24PC:admin#
```

To configure the AP in rogue mode:

```
DWS-3160-24PC:admin#config wireless ap_database 00-22-B0-3C-DD-C0 mode rogue
Command: config wireless ap_database 00-22-B0-3C-DD-C0 mode rogue

 AP mode has been changed. The change will not take effect until the AP is
reboot.

Success.

DWS-3160-24PC:admin#
```

87-4 show wireless ap_database

Description

This command is used to display valid AP database entries. If no parameter is specified, then a summary is displayed. When the users enters a MAC address, detailed information of a specific AP will be displayed.

Format

show wireless ap_database {<macaddr>}

Parameters

<macaddr> - (Optional) Enter the AP's Ethernet interface MAC address used here.

Restrictions

None.

Example

To display the wireless AP database table:

```
DWS-3160-24PC:admin#show wireless ap_database
Command: show wireless ap_database

---------------------------------------------------------------------
*             Valid AP  List                                        *
---------------------------------------------------------------------
    MAC Address          Location                       AP Mode
------------------   -----------------------------   ----------------
00-22-B0-3C-DD-C0    5F                                rogue

Total Entries : 1

DWS-3160-24PC:admin#
```

To display a specific AP entry in the AP database:

```
DWS-3160-24PC:admin#show wireless ap_database 00-22-B0-3C-DD-C0
Command: show wireless ap_database 00-22-B0-3C-DD-C0

AP MAC Address                                : 00-22-B0-3C-DD-C0
Location                                      : 5F
AP Mode                                       : rogue
Password Configured                           : no
Profile                                       : 1 - Default
Radio  1 Channel                              : 36
Radio  1 power                                : Auto
Radio  2 Channel                              : Auto
Radio  2 power                                : Auto

DWS-3160-24PC:admin#
```

Chapter 88 Wireless Managed AP Command List

config wireless ap <macaddr> [debug [disable | enable] | radio <int 1-2> {channel <int 1-165> | power <int 1-100>}(1)]
delete wireless ap_neighbors
config wireless ap_download [image_type [img_dwl8600 | img_dwl3600-6600] <url> | group_size <int 1-12> | abort | start [all | <macaddr> | image_type [img_dwl8600 | img_dwl3600-6600]]]
show wireless ap_download
show wireless ap {[<macaddr> {[radio <int 1-2> {[channel | power | radar | statistics | neighbor [ap | client] | vap {<int 0-15> {[statistics]}}]} | statistics | rf_scan {[rogue_classification | triangulation]} | dist_tunnel {statistics}]} | radio | rf_scan]}
reboot wireless ap [<macaddr> | all]
download wireless ap_image image_type [img_dwl8600 | img_dwl3600-6600] tftpserver <ipaddr> src_file <path_filename 64>

88-1 config wireless ap

Description

This command is used to provide management of an access point managed by the Wireless Switch. The new channel, power, debug mode and required password are not saved in the configuration on the Switch. They are only maintained until the next time the AP is discovered.

Format

config wireless ap <macaddr> [debug [disable | enable] | radio <int 1-2> {channel <int 1-165> | power <int 1-100>}(1)]

Parameters

<macaddr> - Enter the Managed AP MAC Address used here.
debug - Specifies to enable or disable the AP debug mode. **disable** - Specifies that the AP debug mode will be disabled. This is the default option. **enable** - Specifies that the AP debug mode will be enabled.
radio - Specifies the radio interface on the managed AP. **<int 1-2>** - Enter the radio interface number used here. This value must be either 1 or 2.
channel - (Optional) Specifies that channel to configure on the managed AP. **<int 1-165>** - Enter the managed AP's channel number here. This value must be between 1 and 165. **power** - (Optional) Specifies the power configured, for the radio, on the managed AP. **<int 1-100>** - Enter the power value used here. This value must be between 1 and 100.

Restrictions

Only Administrators can issue this command.

Example

To enable the AP’s debug mode:

```
DWS-3160-24PC:admin#config wireless ap 00-22-B0-3C-DD-C0 debug enable
Command: config wireless ap 00-22-B0-3C-DD-C0 debug enable

Enter password (32 characters max):*****
Enter the new password again for confirmation:*****
Success.

DWS-3160-24PC:admin#
```

To configure the managed AP’s channel:

```
DWS-3160-24PC:admin#config wireless ap 00-22-B0-3C-DD-C0 radio 1 channel 36
Command: config wireless ap 00-22-B0-3C-DD-C0 radio 1 channel 36

Success.

DWS-3160-24PC:admin#
```

To configure the managed AP’s power:

```
DWS-3160-24PC:admin#config wireless ap 00-22-B0-3C-DD-C0 radio 1 power 90
Command: config wireless ap 00-22-B0-3C-DD-C0 radio 1 power 90

Success.

DWS-3160-24PC:admin#
```

88-2 delete wireless ap_neighbors

Description

This command is used to delete entries from the managed AP client and AP neighbor lists.

NOTE: Client neighbor entries added via a client association to the managed AP will not be cleared. These are only removed by the System when a client disassociates.

Format

delete wireless ap_neighbors

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To delete entries from the managed AP client and AP neighbor lists:

```
DWS-3160-24PC:admin#delete wireless ap_neighbors
Command: delete wireless ap_neighbors

Are you sure you want to delete all neighbor entries (both AP and Client) for
all managed APs (y/n) y

All managed AP neighbor entries deleted.

Success.

DWS-3160-24PC:admin#
```

88-3 config wireless ap_download

Description

This command is used to configure the related parameters of an AP code download (Independent AP image download).

Format

config wireless ap_download [image_type [img_dwl8600 | img_dwl3600-6600] <url> | group_size <int 1-12> | abort | start [all | <macaddr> | image_type [img_dwl8600 | img_dwl3600-6600]]]

Parameters

image_type - Specifies the AP image type and the URL for image downloading.
- **img_dwl8600** - Specifies that the AP image type is for the DWL-8600.
- **img_dwl3600-6600** - Specifies that the AP image type is for the DWL-3600 and DWL-6600.
- **<url>** - Enter the AP image URL, used, here. An example is: "tftp://<ipaddress>/<filepath>/<fileName>'.

group_size - Specifies to configure the maximum number of simultaneous AP TFTP server downloads.
- **<int 1-12>** - Enter the group size value here. This value must be between 1 and 12. The default value is 10.

abort - Specifies to abort the current code download on managed APs.

start - Specifies to start the AP code download.
- **all** - Specifies to start the AP code download for all APs.
- **<macaddr>** - Enter the AP's MAC address, to start the AP code download for a specific AP.
- **image_type** - Specifies to start the AP code download for all managed APs, running a specific image type.
  - **img_dwl8600** - Specifies to start the AP code download for all managed APs, running the DWL-8600 image type.
  - **img_dwl3600-6600** - Specifies to start the AP code download for all managed APs, running the DWL-3600 and DWL-6600 image type.

Restrictions

Only Administrators can issue this command.

Example

To configure a URL for the image type DWL-8600AP:

```
DWS-3160-24PC:admin#config wireless ap_download image_type img_dwl8600
tftp://10.254.254.254/dwl8600/8600_D_9_3_1.tar
Command: config wireless ap_download image_type img_dwl8600
tftp://10.254.254.254/dwl8600/8600_D_9_3_1.tar

Success.

DWS-3160-24PC:admin#
```

To configure a URL for the image type DWL-3600AP/DWL-6600AP:

```
DWS-3160-24PC:admin#config wireless ap_download image_type img_dwl3600-6600
tftp://10.254.254.254//dwl-ap/3600-6600/6600_D_9_5_3.tar
Command: config wireless ap_download image_type img_dwl3600-6600
tftp://10.254.254.254//dwl-ap/3600-6600/6600_D_9_5_3.tar

Success.

DWS-3160-24PC:admin#
```

To configure an AP code download group size of 12:

```
DWS-3160-24PC:admin#config wireless ap_download group_size 12
Command: config wireless ap_download group_size 12

Success.

DWS-3160-24PC:admin#
```

To start an AP code download for all managed APs running a specific image type:

```
DWS-3160-24PC:admin#config wireless ap_download start image_type img_dwl8600
Command: config wireless ap_download start image_type img_dwl8600

Success.

DWS-3160-24PC:admin#
```

To abort an AP code download:

```
DWS-3160-24PC:admin#config wireless ap_download abort
Command: config wireless ap_download abort

Success.

DWS-3160-24PC:admin#
```

88-4 show wireless ap_download

Description

This command is used to display the global configuration and status of an AP code download request.

Format

show wireless ap_download

Parameters

None.

Restrictions

None.

Example

To display an AP code download configuration and status:

```
DWS-3160-24PC:admin#show wireless ap_download
Command: show wireless ap_download

img_dwl8600 File Name                         : 8600_D_9_3_1.tar
img_dwl8600 File Path                         : dwl8600
img_dwl3600-6600 File Name                    : 6600_D_9_5_3.tar
img_dwl3600-6600 File Path                    : /dwl-ap/3600-6600
Server Address                                : 10.254.254.254
Group Size                                    : 12
Download Type                                 : img_dwl8600
Download Status                               : Failure
Total Count                                   : 2
Success Count                                 : 0
Failure Count                                 : 2
Abort Count                                   : 0
   MAC Address               Location                      Status
-----------------  -----------------------------  -------------------------
00:22:B0:3C:43:C0                                 Failure
00:22:B0:3C:DD:C0                                 Failure

DWS-3160-24PC:admin#
```

88-5 show wireless ap

Description

This command is used to display the operational status for a wireless managed AP. If no parameters are specified, a summary of all managed APs will be displayed.

Format

show wireless ap {[<macaddr> {[radio <int 1-2> {[channel | power | radar | statistics | neighbor [ap | client] | vap {<int 0-15> {[statistics]}}]} | statistics | rf_scan {[rogue_classification | triangulation]} | dist_tunnel {statistics}]} | radio | rf_scan]}

Parameters

<macaddr> - (Optional) Enter the WS managed AP MAC address here. If no parameters are specified, a summary of all managed APs is displayed.

radio - (Optional) Specifies the radio interface on the AP. If no radio ID is specified, a summary of the radio status for all managed APs is displayed.
<int 1-2> - Enter the radio interface ID used here. This value must be between 1 and 2.

channel - (Optional) Specifies to display the manual channel adjustment status for a radio on a WS managed AP. The individual AP status for a wireless channel plan apply request or set request will be displayed.

power - (Optional) Specifies to display the manual power adjustment status for a WS managed AP. The individual AP status for a wireless power plan apply request or set request will be displayed.

radar - (Optional) Specifies to display the radar status for each radio on a WS managed AP. The radar status is displayed for radio modes only. For the b/g mode radios, an error is displayed.

statistics - (Optional) Specifies to display statistics for a managed AP, each physical radio on a WS managed AP, or each VAP on a WS managed AP radio.

neighbor - (Optional) Specifies to display the status for each neighbor AP or client detected through an RF scan on the specified managed AP radio.
ap - Specifies to display the status for each neighbor AP detected through an RF scan on the specified managed AP radio.
client - Specifies to display the status for each client detected as a neighbor to the specified managed AP radio.

vap - (Optional) Specifies the Virtual AP (VAP) ID. If no VAP ID is specified, a summary of all VAPs for a managed AP is displayed.
<int 0-15> - Enter the Virtual AP ID used here. This value must be between 0 and 15.

statistics - (Optional) Specifies to display statistics for a managed AP, each physical radio on a WS managed AP, or each VAP on a WS managed AP radio.

statistics - (Optional) Specifies to display statistics for a managed AP, each physical radio on a WS managed AP, or each VAP on a WS managed AP radio.

rf_scan - (Optional) Specifies to display summarized or detailed information for APs detected via an RF scan on the managed APs. If the optional MAC address parameter is specified, detailed data is displayed.

rogue_classification - (Optional) Specifies to display the WIDS AP rogue classification test results.

triangulation - (Optional) Specifies to display the signal triangulation status for the specified RF scan entry.

dist_tunnel - (Optional) Specifies to display the Layer 2 distributed tunnel status for the specified WS managed AP. If the parameter statistics is specified, the tunnel statistics is displayed.
statistics - Specifies to display the Layer 2 distributed tunnel statistics.

radio - (Optional) Specifies the radio interface on the AP. If no radio ID is specified, a summary of the radio status for all managed APs is displayed.

rf_scan - (Optional) Specifies to display summarized or detailed information for APs detected via an RF scan on the managed APs. If the optional MAC address parameter is specified, detailed data is displayed.

Restrictions

None.

Example

To display the summary status of a managed AP:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0
Command: show wireless ap 00-22-B0-3C-DD-C0

AP MAC Address                     : 00-22-B0-3C-DD-C0
Location                           :
IP Address                         : 192.168.69.126
IP Subnet Mask                     : 255.255.255.0
Managing Switch                    : Local Switch
Switch MAC Address                 : 00-11-22-33-45-67
Switch IP Address                  : 192.168.69.123
Status                             : Managed
Configuration Status               : Success
Last Failing Configuration Element : None
Configuration Failure Error        :
Debug Mode                         : Enabled
Code Download Status               : Failure
Reboot Status                      : Not Started
Profile                            : 1 - Default
Vendor ID                          : D-Link
Protocol Version                   : 2
Software Version                   : 4.0.0.1
Hardware Type                      : DWL-8600AP Dual Radio a/b/g/n
Serial Number                      : H06301226
Part Number                        : dwl8600ap
Discovery Reason                   : L2 Poll Received
Authenticated Clients              : 0
System Up Time                     : 0d:01:15:19
Age                                : 0d:00:00:01

DWS-3160-24PC:admin#
```

To display the summary status of a managed AP on radio 1:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 radio 1
Command: show wireless ap 00-22-B0-3C-DD-C0 radio 1

 MAC address                      : 00-22-B0-3C-DD-C0
 Location                         :
 Radio                            : 1 - 802.11a/n
 Supported Channels               : 36,40,44,48,149,153,157,161,165
 Channel                          : 36
 Channel Bandwidth                : 40 MHz
 Fixed Channel Indicator          : Yes
 Manual Channel Adjustment Status : Success
 Transmit Power                   : 90 %
 Fixed Power Indicator            : Yes
 Manual Power Adjustment Status   : Success
 Authenticated Clients            : 0
 Total Neighbors                  : 1
 WLAN Utilization                 : 0

DWS-3160-24PC:admin#
```

To display the channel status of a managed AP on radio 1:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 radio 1 channel
Command: show wireless ap 00-22-B0-3C-DD-C0 radio 1 channel

 Manual Channel Adjustment Status : Success
 Channel                          : 36

DWS-3160-24PC:admin#
```

To display the power status of a managed AP on radio 1:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 radio 1 power
Command: show wireless ap 00-22-B0-3C-DD-C0 radio 1 power

 Manual Power Adjustment Status : Success
 Transmit Power                 : 90 %

DWS-3160-24PC:admin#
```

To display the radar status of a managed AP on radio 1:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 radio 1 radar
Command: show wireless ap 00-22-B0-3C-DD-C0 radio 1 radar

           Radar Detection    Radar Detected     Last Radar
 Channel      Required            Status        Detected Time
 ------- ------------------- ---------------- ----------------
 36      No                  No               0d:00:00:00
 40      No                  No               0d:00:00:00
 44      No                  No               0d:00:00:00
 48      No                  No               0d:00:00:00
 149     No                  No               0d:00:00:00
 153     No                  No               0d:00:00:00
 157     No                  No               0d:00:00:00
 161     No                  No               0d:00:00:00
 165     No                  No               0d:00:00:00

DWS-3160-24PC:admin#
```

To display the neighbor APs of a managed AP on radio 1:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 radio 1 neighbor ap
Command: show wireless ap 00-22-B0-3C-DD-C0 radio 1 neighbor ap

 MAC address : 00-22-B0-3C-DD-C0
 Location    :
 Radio       : 1 - 802.11a/n

 Neighbor AP MAC   SSID                     RSSI Status          Age
 ----------------- ------------------------ ---- --------------- --------------
 00-22-B0-3C-43-C0 DWS01                    12   Rogue           0d:00:06:20

Total Neighbor APs: 1

DWS-3160-24PC:admin#
```

To display the neighbor clients of a managed AP on radio 1:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 radio 1 neighbor client
Command: show wireless ap 00-22-B0-3C-DD-C0 radio 1 neighbor client

 MAC address : 00-22-B0-3C-DD-C0
 Location    :
 Radio       : 1 - 802.11a/n
 No neighbor clients exist.

DWS-3160-24PC:admin#
```

To display the summary VAP status of a managed AP on radio 1:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 radio 1 vap
Command: show wireless ap 00-22-B0-3C-DD-C0 radio 1 vap

 MAC address : 00-22-B0-3C-DD-C0
 Location    :
 Radio       : 1 - 802.11a/n
                                                     Client
 VAP ID   VAP MAC Address            SSID            Auth.
 ------ ------------------ ------------------------ ------
 0      00-22-B0-3C-DD-C0   dlink1                   0
 1      00-22-B0-3C-DD-C1   dlink2                   0
 2      00-22-B0-3C-DD-C2   dlink3                   0
 3      00-22-B0-3C-DD-C3   dlink4                   0
 4      00-22-B0-3C-DD-C4   dlink5                   0
 5      00-22-B0-3C-DD-C5   dlink6                   0
 6      00-22-B0-3C-DD-C6   dlink7                   0
 7      00-22-B0-3C-DD-C7   dlink8                   0
 8      00-22-B0-3C-DD-C8   dlink9                   0
 9      00-22-B0-3C-DD-C9   dlink10                  0
 10     00-22-B0-3C-DD-CA   dlink11                  0
 11     00-22-B0-3C-DD-CB   dlink12                  0
 12     00-22-B0-3C-DD-CC   dlink13                  0
 13     00-22-B0-3C-DD-CD   dlink14                  0
 14     00-22-B0-3C-DD-CE   dlink15                  0
 15     00-22-B0-3C-DD-CF   dlink16                  0

DWS-3160-24PC:admin#
```

To display the detailed status of a managed AP on radio 1 VAP 1:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 radio 1 vap 1
Command: show wireless ap 00-22-B0-3C-DD-C0 radio 1 vap 1

 MAC address            : 00-22-B0-3C-DD-C0
 Location               :
 Radio                  : 1 - 802.11a/n
 VAP ID                 : 1
 VAP MAC Address        : 00-22-B0-3C-DD-C1
 SSID                   : dlink2
 Client Authentications : 0

DWS-3160-24PC:admin#
```

To display the detailed statistics of a managed AP on radio 1 VAP 1:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 radio 1 vap 1 statistics
Command: show wireless ap 00-22-B0-3C-DD-C0 radio 1 vap 1 statistics

 MAC address                    : 00-22-B0-3C-DD-C0
 Location                       :
 Radio                          : 1 - 802.11a/n
 VAP ID                         : 1
 WLAN Packets Received          : 0
 WLAN Packets Transmitted       : 0
 WLAN Bytes Received            : 0
 WLAN Bytes Transmitted         : 0
 WLAN Packets Receive Dropped   : 0
 WLAN Packets Transmit Dropped  : 0
 WLAN Bytes Receive Dropped     : 0
 WLAN Bytes Transmit Dropped    : 0
 Client Association Failures    : 0
 Client Authentication Failures : 0

DWS-3160-24PC:admin#
```

To display the detailed statistics of a managed AP on radio 1:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 radio 1 statistics
Command: show wireless ap 00-22-B0-3C-DD-C0 radio 1 statistics

 MAC address                   : 00-22-B0-3C-DD-C0
 Location                      :
 Radio                         : 1 - 802.11a/n
 WLAN Packets Received         : 0
 WLAN Packets Transmitted      : 1808
 WLAN Bytes Received           : 0
 WLAN Bytes Transmitted        : 208808
 WLAN Packets Receive Dropped  : 0
 WLAN Packets Transmit Dropped : 0
 WLAN Bytes Receive Dropped    : 0
 WLAN Bytes Transmit Dropped   : 0
 Fragments Received            : 43505
 Fragments Transmitted         : 1808
 Multicast Frames Received     : 0
 Multicast Frames Transmitted  : 1808
 Duplicate Frame Count         : 0
 Failed Transmit Count         : 0
 Transmit Retry Count          : 0
 Multiple Retry Count          : 0
 RTS Success Count             : 0
 RTS Failure Count             : 0
 ACK Failure Count             : 0
 FCS Error Count               : 29
 Frames Transmitted            : 1808
 WEP Undecryptable Count       : 0

DWS-3160-24PC:admin#
```

To display the summary statistics of a managed AP:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 statistics
Command: show wireless ap 00-22-B0-3C-DD-C0 statistics

 MAC address                                      : 00-22-B0-3C-DD-C0
 Location                                         :
 WLAN Packets Received                            : 0
 WLAN Packets Transmitted                         : 3628
 WLAN Bytes Received                              : 0
 WLAN Bytes Transmitted                           : 418436
 WLAN Packets Receive Dropped                     : 0
 WLAN Packets Transmit Dropped                    : 0
 WLAN Bytes Receive Dropped                       : 0
 WLAN Bytes Transmit Dropped                      : 0
 Ethernet Packets Received                        : 1425
 Ethernet Packets Transmitted                     : 2707
 Ethernet Bytes Received                          : 181479
 Ethernet Bytes Transmitted                       : 1531606
 Ethernet Multicast Packets Received              : 357
 Total Transmit Errors                            : 0
 Total Receive Errors                             : 0
 ARP Reqs Converted from Bcast to Ucast           : 0
 Filtered ARP Requests                            : 0
 Broadcasted ARP Requests                         : 0

DWS-3160-24PC:admin#
```

To display the RF scan status of a managed AP:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 rf_scan
Command: show wireless ap 00-22-B0-3C-DD-C0 rf_scan

 MAC Address                              : 00-22-B0-3C-DD-C0
 SSID                                     : dlink1
 OUI                                      : D-Link Corporation
 BSSID                                    : 00-22-B0-3C-DD-C0
 Physical Mode                            : 802.11a/n
 Channel                                  : 36
 Status                                   : Managed
 Initial Status                           : Managed
 AP MAC Address                           : 00-22-B0-3C-DD-C0
 Radio                                    : 1 - 802.11a/n
 Transmit Rate (Mbps)                     : 60
 Beacon Interval (msecs)                  : 100
 Discovered Age                           : 0d:01:02:23
 Age                                      : 0d:00:17:23
 Security Mode                            : Open
 Highest supported rate (Mbps)            : 144.4 Mbps
 802.11n Mode                             : Supported
 Ad hoc Network                           : Not Ad hoc
 Peer Managed AP                          : Managed by the local switch
 Rogue Mitigation                         : Not Required

DWS-3160-24PC:admin#
```

To display the RF scan rogue classification information of a managed AP:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 rf_scan
rogue_classification
Command: show wireless ap 00-22-B0-3C-DD-C0 rf_scan rogue_classification

              Cond                        Test   Test   Time Since  Time Since
Test ID       Detect   MAC Addr (radio)   Config Result 1st Report  Last Report
------------- ------ -------------------- ------ ------ ----------- -----------
WIDSAPROGUE01 False 00-00-00-00-00-00(0) Enable         0d:00:00:00 0d:00:00:00
WIDSAPROGUE02 False 00-00-00-00-00-00(0) Enable         0d:00:00:00 0d:00:00:00
WIDSAPROGUE03 False 00-00-00-00-00-00(0) Enable         0d:00:00:00 0d:00:00:00
WIDSAPROGUE04 False 00-00-00-00-00-00(0) Enable         0d:00:00:00 0d:00:00:00
WIDSAPROGUE05 False 00-00-00-00-00-00(0) Enable         0d:00:00:00 0d:00:00:00
WIDSAPROGUE06 False 00-00-00-00-00-00(0) Enable         0d:00:00:00 0d:00:00:00
WIDSAPROGUE07 False 00-00-00-00-00-00(0) Enable         0d:00:00:00 0d:00:00:00
WIDSAPROGUE08 False 00-00-00-00-00-00(0) Enable         0d:00:00:00 0d:00:00:00
WIDSAPROGUE09 False 00-00-00-00-00-00(0) Enable         0d:00:00:00 0d:00:00:00
WIDSAPROGUE11 False 00-00-00-00-00-00(0) Enable         0d:00:00:00 0d:00:00:00

WIDSAPROGUE01 Administrator configured rogue AP
WIDSAPROGUE02 Managed SSID from an unknown AP
WIDSAPROGUE03 Managed SSID from a fake managed AP
WIDSAPROGUE04 AP without an SSID
WIDSAPROGUE05 Fake managed AP on an invalid channel
WIDSAPROGUE06 Managed SSID detected with incorrect security
WIDSAPROGUE07 Invalid SSID from a managed AP
WIDSAPROGUE08 AP is operating on an illegal channel
WIDSAPROGUE09 Standalone AP with unexpected configuration
WIDSAPROGUE11 Unmanaged AP detected on wired network

DWS-3160-24PC:admin#
```

To display the RF scan triangulation information of a managed AP:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 rf_scan triangulation
Command: show wireless ap 00-22-B0-3C-DD-C0 rf_scan triangulation

                                   RSSI Signal Noise
  Sentry      MAC Address    Radio (%)  (dBm)  (dBm) Age
---------- ----------------- ----- ---- ------ ----- -----------
Non-Sentry 00-22-B0-3C-43-C0   1     15    -80   -91 0d:00:17:50

DWS-3160-24PC:admin#
```

To display AP distributed tunnel statistics:

```
DWS-3160-24PC:admin#show wireless ap 00-22-B0-3C-DD-C0 dist_tunnel statistics
Command: show wireless ap 00-22-B0-3C-DD-C0 dist_tunnel statistics

MAC address                                       : 00-22-B0-3C-DD-C0
Distributed Tunnel Bytes Transmitted              : 0
Distributed Tunnel Packets Transmitted            : 0
Distributed Tunnel Multicast Packets Transmit     : 0
Distributed Tunnel Bytes Received                 : 0
Distributed Tunnel Packets Received               : 0
Distributed Tunnel Multicast Packets Received     : 0
Distributed Tunnel Roamed Clients of AP           : 0
Distributed Tunnel Roamed Clients Idle Timed      : 0
Distributed Tunnel Roamed Clients Age Timed       : 0
Distributed Tunnel Client Limit Denials           : 0
Distributed Tunnel Client Max Replication Denials : 0

DWS-3160-24PC:admin#
```

To display the summary of all managed APs:

```
DWS-3160-24PC:admin#show wireless ap
Command: show wireless ap

MAC Address                                        Configuration
(*) Peer Managed     IP Address    Profile Status     Status           Age
------------------ --------------- ------- ------- ------------- --------------
*00-22-B0-3C-43-C0  192.168.69.125 1       Managed Success       0d:00:00:04
 00-22-B0-3C-DD-C0  192.168.69.126 1       Managed Success       0d:00:00:05

Total Entries : 2

DWS-3160-24PC:admin#
```

To display the radio summary of all managed APs:

```
DWS-3160-24PC:admin#show wireless ap radio
Command: show wireless ap radio

    MAC Address                                       Transmit   Auth.
 (*) Peer Managed       Location        Radio Channel Power (%) Clients
------------------ -------------------- ----- ------- --------- -------
*00-22-B0-3C-43-C0                       1     36      100       0
                                         2     6       100       0
 00-22-B0-3C-DD-C0
                                         1     36      90        0
                                         2     1       100       0

Total APs : 2

DWS-3160-24PC:admin#
```

To display the RF scan summary of all managed APs:

```
DWS-3160-24PC:admin#show wireless ap rf_scan
Command: show wireless ap rf_scan


                                                       Physical
   MAC Address          SSID           Mode     Chan    Status         Age
----------------- ----------------  ----------- ---- ------------ -------------
00-00-B0-F0-C8-AA dlink             802.11b/g   6    Unknown      0d:00:00:28
00-03-7F-BE-F1-37                   802.11a     36   Rogue        0d:00:00:28
00-03-7F-BE-F1-38                   802.11b/g   6    Rogue        0d:00:00:28
00-05-5D-55-94-A0 jamesg            802.11b/g   9    Unknown      0d:00:51:29
00-11-95-95-CA-18 SD1VAPB0          802.11b/g   1    Unknown      0d:00:10:07
00-15-E9-C3-EB-69 NataliexTest      802.11b/g   6    Unknown      0d:00:00:28
00-18-02-6D-B3-62 SD5               802.11b/g   4    Unknown      0d:00:45:29
00-22-B0-3C-43-C0 DWS01             802.11a/n   36   Rogue        0d:00:09:07
00-22-B0-3C-DD-C0 dlink1            802.11a/n   36   Managed      0d:00:00:28
00-22-B0-FF-E9-00                   802.11b/g   6    Rogue        0d:00:00:28
00-26-5A-9D-BE-B0 Steven_AP         802.11b/g   6    Unknown      0d:00:00:28
00-50-BA-00-00-C8 Innit             802.11b/g   6    Unknown      0d:00:00:28
00-62-35-25-55-08 2555 Test         802.11b/g   6    Unknown      0d:00:00:28
00-E0-4C-81-96-C1 BT_Real           802.11b/g   1    Unknown      0d:00:21:37
02-62-35-25-55-08 marg guest        802.11b/g   6    Unknown      0d:00:00:28
06-11-95-95-CA-18 SD1VAPB1          802.11b/g   1    Unknown      0d:00:55:07
1C-00-02-25-55-20 James2555         802.11b/g   9    Unknown      0d:00:18:29
1C-05-5D-55-93-80 hank2555x12       802.11b/g   6    Unknown      0d:00:00:28
1C-18-02-6D-B2-E0 kaycloudAP        802.11b/g   10   Unknown      0d:00:28:30
1C-7E-E5-97-F6-A4 dlink_DWR-112     802.11b/g   6    Unknown      0d:00:00:29
1E-00-02-25-55-20 james2555guest    802.11b/g   9    Unknown      0d:00:18:30
1E-05-5D-55-93-80 hankguest         802.11b/g   6    Unknown      0d:00:00:29
1E-18-02-6D-B2-E0 kayguest          802.11b/g   10   Unknown      0d:00:40:30
5C-22-B0-FF-E8-30                   802.11b/g   6    Rogue        0d:00:00:29
F0-7D-68-82-85-F4 dlink             802.11b/g   9    Unknown      0d:00:40:30

Total Entries : 25

DWS-3160-24PC:admin#
```

In the above examples the following display parameters can be noticed:

MAC Address - Displays the Ethernet address of the WS managed AP.

Location - Displays the location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).

IP Address - Displays the network IP address of the managed AP.

IP Subnet Mask - Displays the network mask of the managed AP.

Managing Switch - Displays whether the AP is managed by this Wireless Switch or a peer Wireless Switch.

Switch MAC Address - Displays the Ethernet address of the Wireless Switch managing the AP.

Switch IP Address - Displays the network IP address of the Wireless Switch managing the AP.

Status - Displays the current managed state of the AP. The possible values are:

Discovered - The AP is discovered by the switch, but is not yet authenticated.

Upgrading - The AP has been validated. The AP code image is upgraded as it does not match the version stored on the wireless switch. This status displays only if the Integrated AP Image Mode is supported by the wireless switch.

Authenticated - The AP has been validated and authenticated (if authentication is enabled), but it is not configured.

Managed - The AP profile configuration has been applied to the AP and it is operating in managed mode.

Failed - The Unified Switch lost contact with the AP. A failed entry will remain in the managed AP database unless you remove it. Note that a managed AP will temporarily show a failed status during a reboot.

Configuration Status - Displays if the AP is configured successfully with the assigned profile.

Last Failing Configuration Element - Displays the element ID of the last failing configuration element. If the configuration status indicates a partial or complete failure, this field indicates the last element that failed during configuration.

Configuration Failure Error - Displays an ASCII string provided by the AP containing an error message for the last failing configuration element.

Debug Mode - Displays whether or not debug mode is enabled on the AP. Debug mode allows you telnet access to the device.

Code Download Status - Displays the current status of a code download request for this AP.

Reboot Status - Displays the current status of an AP rebooting, if one has been initiated.

Profile - Displays the AP profile configuration currently applied to the managed AP, the profile is assigned to the AP in the valid AP database. Note: Once an AP is discovered and managed by the Unified Switch, if the profile is changed in the valid AP database (either locally or on the RADIUS server) the AP must be rebooted to configure with the new profile.

Vendor ID - Displays the Vendor of the AP software, this is learned from the AP during discovery.

Protocol Version - Displays the protocol version supported by the software on the AP. This is learned from the AP during discovery.

Software Version - Displays the version of software on the AP. This is learned from the AP during discovery.

Hardware Type - Displays the Hardware platform for the AP. This is learned from the AP during discovery.

Serial Number - Displays the Unique Serial number assigned to the AP. This is learned from the AP during discovery.

Part Number - Displays the Hardware part number for the AP. This is learned from the AP during discovery.

Access Category - Displays the access category to which the following values pertain.

Number of Active Traffic Streams - Displays the current number of traffic streams for the designated access category of the WS managed AP.

Number of Traffic Stream Clients - Displays the current number of wireless clients with at least one traffic stream for the designated access category of the WS managed AP.

Number of Traffic Stream Roaming Clients - Displays the current number of wireless roaming clients with at least one traffic stream for the designated access category of the WS managed AP. This value is included in the Num Traffic Stream Clients listed above.

Radio - Displays the radio interface on the AP.

Channel - Displays the current operating channel for the radio.

Bandwidth - Displays the current channel bandwidth in use.

Transmit Power - Displays the current channel bandwidth in use. If the radio is operational, the current transmit power for the radio.

Associated Clients - Displays the total count of clients associated on the physical radio, this is a sum of all the clients associated to each VAP enabled on the radio.

Total Neighbors - Displays the total number of neighbors (both APs and clients) that can be seen by this radio in its RF area.

Supported Channels - Displays the list of eligible channels the AP reported to the switch for channel assignment. This list is based on country code, hardware capabilities, and any configured channel limitations.

Fixed Channel Indicator - Displays whether a fixed channel is configured and assigned to the radio. A fixed channel can be configured in the valid AP database (locally or on a RADIUS server).

Manaual Channel Adjustment Status - Displays the current state of a manual request to change the channel on this radio.

Fixed Power Indicator - Displays the fixed power setting configured and assigned to the radio. A fixed transmit power can be configured in the valid AP database (locally or on a RADIUS server).

Manual Power Adjustment Status - Displays the state of a manual request to change the power setting on this radio.

WLAN Utilization - Displays the total network utilization for the physical radio. This value is based on radio statistics.

Medium Time Unallocated - Displays the amount of configured medium time available for non-roaming and roaming clients for the designated access category on this radio. This value is in units of 32 microseconds-per-second (usecs/sec).

Medium Time Roaming Unallocated - Displays the amount of configured medium time available for roaming clients only for the designated access category on this radio. This value is in units of 32 microseconds-per-second (usecs/sec).

VAP ID - Displays the integer ID used to identify the VAP (0-7), this is used to uniquely identify the VAP for configuration via CLI/SNMP.

VAP MAC Address - Displays the Ethernet address of the VAP.

SSID - Displays the network assigned to the VAP. The network for each VAP is configured within the AP profile and the SSID is based on the network configuration.

Client Assoc - Displays the total number of clients currently associated to the VAP.

Operational Status - Displays the current operational status of the designated access category on this VAP.

Neighbor AP MAC - Displays the Ethernet MAC address of the neighbor AP network, this could be a physical radio interface or VAP MAC address. For Broadcom APs, this is always a VAP MAC address. The neighbor AP MAC address may be cross-referenced in the RF Scan status.

RSSI - Displays the Received Signal Strength Indication, this is an indicator of the signal strength relative to the neighbor and may give an idea of the neighbor's distance from the managed AP.

Status - Displays the managed status of the AP, whether this is a valid AP known to the switch or a Rogue on the network. The valid values are:

Managed - The neighbor AP is managed by this switch or another switch within the peer group. The neighbor AP status can be referenced using its base MAC address.

Unknown- The neighbor APs detected in the RF scan are initially categorized as "Unknown" APs.

Standalone - The AP is managed in standalone mode and configured as a valid AP entry (local or RADIUS).

Rogue - The AP intrusion Detection function has determined that the AP is posing a threat to the network and categorizes the neighbor AP as rogue.

Age - Displays the time since this AP or client was last reported from an RF scan on the radio.

Discovery Reason - Displays one or more discovery methods for the neighbor client. One of more of the following abbreviated values may be displayed:

RF Scan (RF) - The client was reported from an RF scan on the radio. Note that client stations are difficult to detect via RF scan; the other methods are more common for client neighbor detection.

Probe Request (Probe) - The managed AP received a probe request from the client.

Associated to Managed AP (Assoc Managed AP) - This neighbor client is associated to another managed AP.

Associated to this AP (Assoc this AP) - The client is associated to this managed AP on the displayed radio.

Associated to Peer AP (Assoc peer AP) - The client is associated to a peer switch managed AP.

Ad Hoc Rogue (Ad Hoc) - The client was detected as part of an Ad Hoc network.

WLAN Packets Received - Displays the total packets received by the AP on the wireless network.

WLAN Bytes Received - Displays the total bytes received by the AP on the wireless network.

WLAN Packets Transmitted - Displays the total packets transmitted by the AP on the wireless network.

WLAN Bytes Transmitted - Displays the total bytes transmitted by the AP on the wireless network.

WLAN Packets Receive Dropped - Displays the total receive packets discarded by the AP on the wireless network.

WLAN Bytes Received Dropped - Displays the total receive bytes discarded by the AP on the wireless network.

WLAN Packets Transmitted Dropped - Displays the total packets discarded by the AP prior to transmission on the wireless network.

WLAN Bytes Transmitted Dropped - Displays the total bytes discarded by the AP prior to transmission on the wireless network.

Ethernet Packets Received - Displays the total packets received by the AP on the wired network.

Ethernet Bytes Received - Displays the total bytes received by the AP on the wired network.

Ethernet Multicast Packets Received - Displays the total multicast packets received by the AP on the wired network.

Ethernet Packets Transmitted - Displays the total packets transmitted by the AP on the wired network.

Ethernet Bytes Transmitted - Displays the total bytes transmitted by the AP on the wired network.

Total Transmit Errors - Displays the total transmit errors detected by the AP on the wired network.

Total Receive Errors - Displays the total receive errors detected by the AP on the wired network.

ARP Reqs converted from Bcast to Ucast - Displays the total number of ARP request converted from broadcast to unicast on the wireless network.

Filtered ARP Requests - Displays the total number of ARP requests filtered by the AP instead of sending on the wireless network.

Broadcasted ARP Requests - Displays the total number of ARP requests broadcasted on the wireless network after performing wireless ARP suppression.

Transmitted Fragment Count - Displays the count of acknowledged MPDU with an individual address or an MPDU with a multicast address of type Data or Management.

Multicast Transmitted Frame Count - Displays the count of successfully transmitted MSDU frames where the multicast bit is set in the destination MAC address.

Failed Count - Displays the number of times a MSDU is not transmitted successfully due to transmit attempts exceeding either the short retry limit or the long retry limit.

Retry Count - Displays the number of time a MSDU is successfully transmitted after one or more retries.

Multiple Retry Count - Displays the number of times a MSDU is successfully transmitted after more than one retry.

Frame Duplicated Count - Displays the number of times a frame is received and the Sequence Control field indicates it is a duplicate.

RTS Success Count - Displays the count of CTS frames received in response to an RTS frame.

RTS Failure Count - Displays the count of CTS frames not received in response to an RTS frame.

ACK Failure Count - Displays the count of ACK frames not received when expected.

Received Fragment Count - Displays the count of successfully received MPDU frames of type data or management.

Multicast Received Frame Count - Displays the count of MSDU frames received with the multicast bit set in the destination MAC address.

FCS Error Count - Displays the count of FCS errors detected in a received MPDU frame.

Transmitted Frame Count - Displays the count of each successfully transmitted MSDU.

WEP Undecryptable Count - Displays the count of encrypted frames received and the key configuration of the transmitter indicates that the frame should not have been encrypted or that frame was discarded due to the receiving station not implementing the privacy option.

Client Association Failures - Displays the number of clients that have been denied association to the VAP.

Client Authentication Failures - Displays the number of clients that have failed authentication to the VAP.

Radar Detection Required - Displays whether the radar detection is required on some channels in the 5 GHz band. If radar detection is required on the channel, the AP uses the 802.11h specification to avoid interference with other wireless devices.

Radar Detected Status - Displays whether another 802.11 device was detected on the channel.

Last Radar Detected Time - Displays the amount of time that has passed since the device was last detected on the channel.

88-6 reboot wireless ap

Description

This command is used to request the Switch to reboot all the managed APs or the managed AP indicated by the MAC address.

Format

reboot wireless ap [<macaddr> | all]

Parameters

<macaddr> - Enter the Managed AP MAC address here.
all - Specifies that all the managed APs will be rebooted.

Restrictions

Only Administrators can issue this command.

Example

To reboot all the managed APs:

```
DWS-3160-24PC:admin#reboot wireless ap all
Command: reboot wireless ap all

Are you sure you want to reboot all WS managed APs? (y/n) y
Reboot Requested for all WS managed APs.

Success.

DWS-3160-24PC:admin#
```

88-7 download wireless ap_image image_type

Description

This command is used to initiate an AP code image file download process, to the wireless Switch.

Format

download wireless ap_image image_type [img_dwl8600 | img_dwl3600-6600] tftpserver <ipaddr> src_file <path_filename 64>

Parameters

image_type - Specifies the AP image type to be configured for downloading.
img_dwl8600 - Specifies that the AP image type will be for the DWL-8600.
img_dwl3600-6600 - Specifies that the AP image type will be for the DWL-3600 and the DWL-6600.

tftpserver - Specifies the IP address of the TFTP server.
<ipaddr> - Enter the IP address, of the TFTP server, here.

src_file - Specifies source path and filename of the image file on the TFTP server.
<path_filename 64> - Enter the source path and filename, of the file on the TFTP server,

	here. This string can be up to 64 characters long.

Restrictions

Only Administrators can issue this command.

Example

To download an image file from the DWL-8600AP to the Switch, through TFTP:

```
DWS-3160-24PC:admin# download wireless ap_image image_type img_dwl8600
tftpserver 192.168.69.66 src_file d:/apimage.tar
Command: download wireless ap_image image_type img_dwl8600 tftpserver
192.168.69.66 src_file d:/apimage.tar


 Connecting to server................... Done.
 Download AP image...................... 100 %
 Download AP image process.............. Done.


DWS-3160-24PC:admin#
```

Chapter 89 Wireless Network Command List

create wireless network <int 1-64>

delete wireless network <int 1-64>

config wireless network <int 1-64> [arp_suppression [enable | disable] | clear | client_qos [state [enable | disable] | access_control [down | up] [ip [acl_num <int 1-199> | acl_name <name 31>] | ipv6 acl_name <name 31> | mac acl_name <name 31> | clear] | bandwidth_limit [down | up] [<uint 0-4294967295> | default] | diffserv_policy [down | up] [policy_name <name 31> | clear]] | deny_broadcast [enable | disable] | dist_tunnel [enable | disable] | dot1x [bcast_key_refresh_rate <int 0-86400> | session_key_refresh_rate <int>] | hide_ssid [enable | disable] | mac_authentication [enable [local | radius] | disable] | radius [accounting [enable | disable] | use_network_configuration [enable | disable]] | redirect [mode [http | none | default] | url [<url> | clear]] | security mode [none | static_wep | wep_dot1x | wpa_enterprise | wpa_personal | default] | ssid <ssid 32> | vlan [<int 1-4094> | default] | wep [authentication [open_system {shared_key} | shared_key | default] | key [index <int 1-4> [value <string> | clear] | length [64 | 128 | default] | type [ascii | hex | default]] | tx_key [<int 1-4> | default]] | wpa [ciphers [ccmp {tkip} | tkip | default] | key [value <string> | clear] | versions [wpa {wpa2} | wpa2 | default]] | wpa2 [key_chching holdtime [<int 1-1440> | default] | pre_authentication [state [enable | disable] | limit [<int 0-192> | default]]] | ip_tunnel [state [enable | disable] | subnet <ipaddr> mask <netmask>]]

show wireless network {<int 1-64>}

89-1 create wireless network

Description

This command is used to add a wireless network configuration.

Format

create wireless network <int 1-64>

Parameters

<int 1-64> - Enter the new wireless network ID used here. This value must be between 1 and 64. Sixteen networks are created by default. The Switch supports up to 64 networks.

Restrictions

Only Administrators can issue this command.

Example

To create a wireless network configuration:

```
DWS-3160-24PC:admin#create wireless network 17
Command: create wireless network 17

 Create Network ID : 17

Success.

DWS-3160-24PC:admin#
```

89-2 delete wireless network

Description

This command is used to delete a wireless network configuration. If a network is applied to one or more VAPs within an AP profile, it cannot be deleted. The first sixteen default networks can never be deleted.

Format

delete wireless network <int 1-64>

Parameters

<int 1-64> - Enter the wireless network ID, that will be deleted, here. This value must be between 1 and 64.

Restrictions

Only Administrators can issue this command.

Example

To delete a wireless network configuration:

```
DWS-3160-24PC:admin#delete wireless network 17
Command: delete wireless network 17

 Delete Network ID : 17.

Success.

DWS-3160-24PC:admin#
```

89-3 config wireless network

Description

This command is used to configure a wireless networks configuration.

Format

config wireless network <int 1-64> [arp_suppression [enable | disable] | clear | client_qos [state [enable | disable] | access_control [down | up] [ip [acl_num <int 1-199> | acl_name <name 31>] | ipv6 acl_name <name 31> | mac acl_name <name 31> | clear] | bandwidth_limit

[down | up] [<uint 0-4294967295> | default] | diffserv_policy [down | up] [policy_name <name 31> | clear]] | deny_broadcast [enable | disable] | dist_tunnel [enable | disable] | dot1x [bcast_key_refresh_rate <int 0-86400> | session_key_refresh_rate <int>] | hide_ssid [enable | disable] | mac_authentication [enable [local | radius] | disable] | radius [accounting [enable | disable] | use_network_configuration [enable | disable]] | redirect [mode [http | none | default] | url [<url> | clear]] | security mode [none | static_wep | wep_dot1x | wpa_enterprise | wpa_personal | default] | ssid <ssid 32> | vlan [<int 1-4094> | default] | wep [authentication [open_system {shared_key} | shared_key | default] | key [index <int 1-4> [value <string> | clear] | length [64 | 128 | default] | type [ascii | hex | default]] | tx_key [<int 1-4> | default]] | wpa [ciphers [ccmp {tkip} | tkip | default] | key [value <string> | clear] | versions [wpa {wpa2} | wpa2 | default]] | wpa2 [key_chching holdtime [<int 1-1440> | default] | pre_authentication [state [enable | disable] | limit [<int 0-192> | default]]] | ip_tunnel [state [enable | disable] | subnet <ipaddr> mask <netmask>]]

Parameters

<int 1-64> - Enter the wireless network ID used here. This value must be between 1 and 64.

arp_suppression - Specifies the state of the mode that allows the APs to reduce the number of broadcasted ARP requests on the wireless interfaces. Reducing broadcasts helps to conserve power on the wireless clients. The wireless clients that utilize the power-save mode must then wake up and use more power when they detect broadcasted frames. Enabling this feature slightly degrades AP packet forwarding performance due to extra packet filtering that takes place to find DHCP packets and extra processing for ARP request and reply packets. Networks that do not use IPv4 should not enable this feature.

enable - Specifies that the state of the mode, that allows the APs to reduce the number of broadcasted ARP requests on the wireless interfaces, will be enabled.

disable - Specifies that the state of the mode, that allows the APs to reduce the number of broadcasted ARP requests on the wireless interfaces, will be disabled. This is the default option.

clear - Specifies to restores a network configuration to its default values.

client_qos - Specifies the client QoS parameters that allows the Switch to apply access control lists (ACLs) and differentiated service (DiffServ) policies to wireless clients, associated with the AP, and extend the Switch QoS features into the wireless domain.

state - Specifies the state of AP client QoS operation for the network. When enabled, clients associated to this network may have one or more of the following QoS facilities in effect in the down and/or up directions: access control, bandwidth limiting, and Differentiated services (via policy).

enable - Specifies that the state of AP client QoS operation for the network will be enabled.

disable - Specifies that the state of AP client QoS operation for the network will be disabled. This is the default option.

access_control - Specifies to configure the ACL used by clients associated with this network.

down - Specifies to select the name of the access list, applied to traffic, in the outbound (down) direction.

up - Specifies to select the name of the access list, applied to traffic, in the inbound (up) direction.

ip acl_num - Specifies to configure IP-standard or IP-extended type of access list to the network as a client QoS.

<int 1-199> - Enter the IP ACL numerical value used here. This value must be between 1 and 199.

acl_name - Specifies to configure the IP-name type of access list to the network as a client QoS.

<name 31> - Enter the IP ACL name value used here. This name can be up to 31 characters long.

ipv6 - Specifies to configure IPv6 type of access list to the network as a client QoS.

acl_name - Specifies to configure the IPv6-name type of access list to the network as a client QoS.

<name 31> - Enter the IPv6 ACL name used here. This name can be up to 31 characters long.

mac - Specifies to configure MAC type of access list to the network as a client QoS.

acl_name - Specifies to configure the MAC-name type of access list to the network as a client QoS.

<name 31> - Enter the MAC ACL name used here. This name can be up to 31 characters long.

clear - Specifies to remove the client QoS access control list parameter configured for this network.

bandwidth_limit - Specifies to configure the default maximum bandwidth rate limit, in bits per second, used by clients associated with this network, that do not obtain their own value via RADIUS. The specified value is subject to rounding down to the nearest 8000 in the AP, with a minimum rounded value of 8000.

down - Specifies the maximum allowed transmission rate from the AP to the wireless client in bits per second.

up - Specifies the maximum allowed client transmission rate to the AP in bits per second.

<uint 0-4294967295> - Enter the client QoS default maximum bandwidth rate limit, for this network, here. This value must be between 0 and 4294967295 bps.

default - Specifies that the default value will be used. The default value is 0.

diffserv_policy - Specifies to configure the Diffserv policy used by clients associated with this network.

down - Specifies to select the name of the DiffServ policy applied to traffic from the AP in the outbound (down) direction.

up - Specifies to select the name of the DiffServ policy applied to traffic sent to the AP in the inbound (up) direction.

policy_name - Specifies to configure the Diffserv policy name to the network as a client QoS.

<name 31> - Enter the Diffserv policy name here. This name can be up to 31 characters long.

clear - Specifies to remove the client QoS default Diffserv policy parameter configured for this network.

---

deny_broadcast - Specifies the state of the deny broadcast mode for the network. If enabled, the AP will not respond to client probe requests broadcasted to all available SSIDs.

enable - Specifies that the state of the deny broadcast mode for the network will be enabled.

disable - Specifies that the state of the deny broadcast mode for the network will be disabled. This is the default option.

---

dist_tunnel - Specifies the state of Layer 2 tunneling for the network. Layer 2 tunneling is recommended when the UWS does not support hardware forwarding acceleration or hardware-based Layer 2 tunnels.

enable - Specifies that the state of Layer 2 tunneling for the network will be enabled.

disable - Specifies that the state of Layer 2 tunneling for the network will be disabled. This is the default option.

---

dot1x - Specifies to configure parameters related to 802.1X.

bcast_key_refresh_rate - Specifies the interval value after which the broadcast keys are changed.

<int 0-86400> - Enter the interval value ,after which the broadcast keys are changed, here. This value must be between 0 and 86400. The default value is 300.

session_key_refresh_rate - Specifies the interval value after which the Unicast session keys are changed.

<int> - Enter the interval value, after which the Unicast session keys are changed, here. The default value is 0.

---

hide_ssid - Specifies the SSID, for this network, will be hidden or not. If enabled, the SSID is not included in the AP beacon frames.

enable - Specifies that the SSID, for this network, will be hidden.

disable - Specifies that the SSID, for this network, will not be hidden. This is the default option.

---

mac_authentication - Specifies the state of MAC authentication on the network. If you enable MAC authentication, wireless clients must be authenticated by the AP in order to connect to the network.

enable - Specifies that MAC authentication, on the network, will be enabled.

local - Specifies that client MAC addresses will use the local database for MAC authentication.

radius - Specifies that client MAC addresses will use the RADIUS database for MAC authentication.

disable - Specifies that MAC authentication, on the network, will be disabled. This is the default option.

radius - Specifies to configure parameters related to RADIUS.

accounting - Specifies the state of RADIUS accounting for wireless clients.

enable - Specifies that RADIUS accounting for wireless clients will be enabled.

disable - Specifies that RADIUS accounting for wireless clients will be disabled. This is the default option.

use_network_configuration - Specifies whether the VAP uses the network RADIUS accounting settings or the global RADIUS settings.

enable - Specifies to use the RADIUS accounting info, defined on the wireless network configuration. This is the default option.

disable - Specifies to use the RADIUS accounting info, defined on the wireless global configuration.

redirect - Specifies the redirection method used.

mode - Specifies the redirection mode used.

http - Specifies to enable HTTP redirection and initial client requests will be redirected to the configured URL.

none - Specifies that HTTP redirection will be disabled. This is the default option.

default - Specifies that the default option will be used.

url - Specifies to configure a URL for HTTP redirection. Note that 'http://' is not entered in the configured URL because this prefix is assumed.

<url> - Enter the URL, used for HTTP redirection, here.

clear - Specifies that the HTTP redirection URL will be cleared.

security mode - Specifies to configure the authentication and encryption mode on the network.

none - Specifies that no authentication or encryption will be used on the wireless network. This is the default option.

static_wep - Specifies that static WEP encryption and authentication will be configured separately.

wep_dot1x - Specifies to use dynamic WEP authentication using 802.1X.

wpa_enterprise - Specifies to use WPA, 802.1X, and authentication.

wpa_personal - Specifies to use WPA, shared-key, authentication.

default - Specifies that the default option will be used.

ssid - Specifies the SSID for the wireless network. A network must be configured with an SSID of one or more characters. The SSID can be modified, but cannot be deleted. Except for the default Guest Network, the default SSID for each network is ‘Managed SSID’ followed by the unique Network ID.

<ssid 32> - Enter the SSID, for the wireless network, here.

vlan - Specifies the default VLAN ID for the network. If there is no RADIUS server configured or a client is not associated with a VLAN via the RADIUS, this will be the VLAN assigned.

<int 1-4094> - Enter the default VLAN ID, for the network, here. This value must be between 1 and 4094. The default value is 1.

default - Specifies that the default option will be used.

wep - Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. If you select this security mechanism, all wireless clients and access points on the network will be configured with a 64-bit shared-key that will be used for data encryption.

authentication - Specifies that the static WEP authentication mode will be used for the wireless network. This value is applicable only when the security mode is configured to use static WEP authentication and encryption.

open_system - Specifies that no authentication is required. This is the default option.

shared_key - (Optional) Specifies that only WEP clients are authenticated.

shared_key - Specifies that clients are required to authenticate to the network using a shared key.

default - Specifies that the default option will be used.

key - Specifies to configure up to 4 static WEP keys for the network. The configured keys are used when the network security mode is set to WEP shared key, according to the configured WEP transfer key index. The number of characters required depends on the configured WEP key type and length.

index - Specifies the configured WEP transfer key index. The number of characters required depends on the configured WEP key type and length.

<int 1-4> - Enter the configured WEP transfer key ID used here. This value must be between 1 and 4.

value - Specifies the WEP key itself, entered in ASCII or HEX format.

<string> - Enter the WEP key here.

clear - Specifies to clear the WEP key entered.

length - Specifies the WEP key length.

64 - Specifies that the WEP key length will be set as 64 bit.

128 - Specifies that the WEP key length will be set as 128 bit. This is the default option.

default - Specifies that the default option will be used.

type - Specifies the WEP key type.

ascii - Specifies that the WEP key type will be set as ASCII.

hex - Specifies that the WEP key type will be set as HEX. This is the default option.

default - Specifies that the default option will be used.

tx_key - Specifies the WEP key index used for encryption on the network. This value is applicable only when the security mode is configured for WEP shared-key authentication and encryption.

<int 1-4> - Enter the WEP key index used here. This value must be between 1 and 4. The default value is 1.

default - Specifies that the default value will be used.

wpa - Specifies that the security mode will be set to WPA.

ciphers - Specifies the WPA cipher suites supported on the network.

ccmp - Specifies that CCMP encryption will be used with WPA.

tkip - (Optional) Specifies that both CCMP and TKIP encryption will be used with WPA. This is the default option.

tkip - Specifies that TKIP encryption will be used with WPA.

default - Specifies that the default option will be used.

key - Specifies the WPA shared-key. This is an alphanumeric string in the range 8-64 characters. The configured key is used when the network security mode is set as WPA shared-key.

value - Specifies the shared secret key for WPA Personal.

<string> - Enter a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include upper and lower case alphabetic letters, numeric digits, and special symbols like '@' and '#'.

clear - Specifies the clear the key entered.

versions - Specifies the WPA version(s) supported on the network. One or both parameters must be specified.

wpa - Specifies the WPA version will be set as WPA.

wpa2 - (Optional) Specifies the WPA version will be set as WPA and WPA2. This is the default option.

wpa2 - Specifies the WPA version will be set as WPA2.

default - Specifies that the default option will be used.

wpa2 - Specifies that the security mode will be set to WPA2.

key_chching - Specifies the length of time a Pairwise Master Key (PMK) will be cached by an AP for either client roaming or key forwarding.

holdtime - Specifies the WPA2 key caching hold time.

<int 1-1440> - Enter the WPA2 key caching hold time here. This value must be between 1 and 1440 minutes. The default value is 10 minutes.

default - Specifies that the default value will be used.

pre_authentication - Specifies that WPA2 pre-authentication support for client roaming will be configured.

state - Specifies the state of WPA2 pre-authentication support for client roaming.

enable - Specifies that WPA2 pre-authentication support for client roaming will be enabled. This is default option.

disable - Specifies that WPA2 pre-authentication support for client roaming will be disabled.

limit - Specifies the WPA2 pre-authentication limit for the network. This specifies a limit on the number of APs within the peer group to which one client is allowed to pre-authenticate.

<int 0-192> - Enter the WPA2 pre-authentication limit, for the network, here. This value must be between 0 and 192. The default value is 0, which means no limit.

default - Specifies that the default value will be used.

ip_tunnel - Specifies the Layer 3 tunnel feature. The Layer 3 Tunnel feature allows mobile stations to maintain their IP connections while roaming from one access point to another access point even when these access points are attached to different IP subnets. When Layer 3 tunneling is enabled the VLAN ID is not used. In fact, the Switch puts the management VLAN ID, if any, on the tunneled packets. If the wireless network topology changes (for example, a UWS reboots) while the Layer 3 tunneling feature is in use, you should perform an ARP refresh on wired clients to speed up the process of re-establishing connectivity to the tunneled network.

state - Specifies the Layer 3 Tunneling option's state. In order for the tunnel to be completely configured, routing must be enabled and the Switch must have a routing interface IP address that is in the tunnel subnet.

enable - Specifies that the Layer 3 tunnel feature will be enabled.

disable - Specifies that the Layer 3 tunnel feature will be disabled. This is the default option.

subnet - Specifies the network IP address subnet used. This field must be in the same subnet as the routing interface for the WLAN, defined on the Switch.

<ipaddr> - Enter the network IP address subnet used here.

mask - Specifies the subnet mask for the network IP address on the Layer 3 tunnel subnet.

<netmask> - Enter the subnet mask for the network IP address on the Layer 3 tunnel subnet here.

Restrictions

Only Administrators can issue this command.

Example

To enable ARP suppression on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 arp_suppression enable
Command: config wireless network 1 arp_suppression enable

Success.

DWS-3160-24PC:admin#
```

To restore Network 1’s configuration to default values:

```
DWS-3160-24PC:admin#config wireless network 1 clear
Command: config wireless network 1 clear

Success.

DWS-3160-24PC:admin#
```

To enable the Client QoS state on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 client_qos state enable
Command: config wireless network 1 client_qos state enable

Success.

DWS-3160-24PC:admin#
```

To configure an IP ACL rule to Client QoS on Network 1:

```
DWS-3160-24PC:admin#create wireless access_list ip standard 1
Command: create wireless access_list ip standard 1

Success.

DWS-3160-24PC:admin#create wireless access_list ip name ipacl
Command: create wireless access_list ip name ipacl

Success.

DWS-3160-24PC:admin#config wireless network 1 client_qos access_control down ip
acl_num 1
Command: config wireless network 1 client_qos access_control down ip acl_num 1

Success.

DWS-3160-24PC:admin#config wireless network 1 client_qos access_control up ip
acl_name ipacl
Command: config wireless network 1 client_qos access_control up ip acl_name
ipacl

Success.

DWS-3160-24PC:admin#
```

To configure a MAC ACL rule to Client QoS on Network 1:

```
DWS-3160-24PC:admin#create wireless access_list mac macacl
Command: create wireless access_list mac macacl

Success.

DWS-3160-24PC:admin#config wireless network 1 client_qos access_control up mac
acl_name macacl
Command: config wireless network 1 client_qos access_control up mac acl_name
macacl

Success.

DWS-3160-24PC:admin#
```

To configure an IPv6 ACL rule to Client QoS on Network 1:

```
DWS-3160-24PC:admin#create wireless access_list ipv6 ipv6acl
Command: create wireless access_list ipv6 ipv6acl

Success.

DWS-3160-24PC:admin#config wireless network 1 client_qos access_control up ipv6
acl_name ipv6acl
Command: config wireless network 1 client_qos access_control up ipv6 acl_name
ip v6acl

Success.

DWS-3160-24PC:admin#
```

To configure the Client QoS bandwidth limit on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 client_qos bandwidth_limit up
11111
Command: config wireless network 1 client_qos bandwidth_limit up 11111

 Granularity of bandwidth limit: 8192 bps.
 Actual up bandwidth Limit: 8192 bps.

Success.

DWS-3160-24PC:admin#
```

To configure a differentiated service (DiffServ) policy to Client QoS on Network 1:

```
DWS-3160-24PC:admin#create wireless diffserv policy_map qos_policy
Command: create wireless diffserv policy_map qos_policy

Success.

DWS-3160-24PC:admin#config wireless network 1 client_qos diffserv_policy down
policy_name qos_policy
Command: config wireless network 1 client_qos diffserv_policy down policy_name
qos_policy

Success.

DWS-3160-24PC:admin#
```

To enable Deny Broadcast on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 deny_broadcast enable
Command: config wireless network 1 deny_broadcast enable

Success.

DWS-3160-24PC:admin#
```

To enable Layer 2 Tunneling on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 dist_tunnel enable
Command: config wireless network 1 dist_tunnel enable

Success.

DWS-3160-24PC:admin#
```

To configure 802.1X Layer 2 Broadcast/Unicast key’s refresh rate on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 dot1x bcast_key_refresh_rate 1234
Command: config wireless network 1 dot1x bcast_key_refresh_rate 1234

Success.

DWS-3160-24PC:admin#config wireless network 1 dot1x session_key_refresh_rate
2345
Command: config wireless network 1 dot1x session_key_refresh_rate 2345

Success.

DWS-3160-24PC:admin#
```

To enable hidden SSID on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 hide_ssid enable
Command: config wireless network 1 hide_ssid enable

Success.

DWS-3160-24PC:admin#
```

To enable MAC Authentication on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 mac_authentication enable local
Command: config wireless network 1 mac_authentication enable local

Success.

DWS-3160-24PC:admin#config wireless network 1 mac_authentication enable radius
Command: config wireless network 1 mac_authentication enable radius

Success.

DWS-3160-24PC:admin#
```

To enable RADIUS accounting on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 radius accounting enable
Command: config wireless network 1 radius accounting enable

Success.

DWS-3160-24PC:admin#
```

To configure the redirect mode on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 redirect mode http
Command: config wireless network 1 redirect mode http

Success.

DWS-3160-24PC:admin#
```

To configure a redirected URL on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 redirect url www.dlink.com
Command: config wireless network 1 redirect url www.dlink.com

Success.

DWS-3160-24PC:admin#
```

To configure the security mode on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 security mode static_wep
Command: config wireless network 1 security mode static_wep

Success.

DWS-3160-24PC:admin#
```

To configure the SSID on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 ssid ssid1
Command: config wireless network 1 ssid "ssid1"

Success.

DWS-3160-24PC:admin#
```

To configure the VLAN on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 vlan 2
Command: config wireless network 1 vlan 2

Success.

DWS-3160-24PC:admin#
```

To configure the WEP authentication mode on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 wep authentication shared_key
Command: config wireless network 1 wep authentication shared_key

Success.

DWS-3160-24PC:admin#
```

To configure the WEP key type on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 wep key type ascii
Command: config wireless network 1 wep key type ascii

Success.

DWS-3160-24PC:admin#
```

To configure the WEP key length on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 wep key length 64
Command: config wireless network 1 wep key length 64

Success.

DWS-3160-24PC:admin#
```

To configure the WEP key value on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 wep key index 1 value wk3y1
Command: config wireless network 1 wep key index 1 value wk3y1

Success.

DWS-3160-24PC:admin#
```

To configure the WEP TX key on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 wep tx_key 2
Command: config wireless network 1 wep tx_key 2

Success.

DWS-3160-24PC:admin#
```

To configure the WPA key ciphers on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 wpa ciphers tkip
Command: config wireless network 1 wpa ciphers tkip

Success.

DWS-3160-24PC:admin#
```

To configure the WPA key version on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 wpa versions wpa2
Command: config wireless network 1 wpa versions wpa2

Success.

DWS-3160-24PC:admin#
```

To configure the WPA key value on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 wpa key value wp4k3y12
Command: config wireless network 1 wpa key value wp4k3y12

Success.

DWS-3160-24PC:admin#
```

To configure the WPA2 key caching hold-time on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 wpa2 key_chching holdtime 1200
Command: config wireless network 1 wpa2 key_chching holdtime 1200

Success.

DWS-3160-24PC:admin#
```

To configure the WPA2 pre-authentication state on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 wpa2 pre_authentication state
enable
Command: config wireless network 1 wpa2 pre_authentication state enable

Success.

DWS-3160-24PC:admin#
```

To configure the WPA2 pre-authentication limit on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 wpa2 pre_authentication limit 120
Command: config wireless network 1 wpa2 pre_authentication limit 120

Success.

DWS-3160-24PC:admin#
```

To configure the Layer 3 tunnel state on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 ip_tunnel state enable
Command: config wireless network 1 ip_tunnel state enable

Success.

DWS-3160-24PC:admin#
```

To configure the Layer 3 tunnel subnet and mask on Network 1:

```
DWS-3160-24PC:admin#config wireless network 1 ip_tunnel subnet 20.20.0.0 mask
255.255.0.0
Command: config wireless network 1 ip_tunnel subnet 20.20.0.0 mask 255.255.0.0

Success.

DWS-3160-24PC:admin#
```

89-4 show wireless network

Description

This command is used to display the network configuration parameters. If no parameter is specified, a summary of the all the configured networks will be displayed.

Format

show wireless network {<int 1-64>}

Parameters

<int 1-64> - (Optional) Enter the Network ID here. This value must be between 1 and 64.

Restrictions

None.

Example

To display a summary of the configured networks:

```
DWS-3160-24PC:admin#show wireless network
Command: show wireless network

Network  SSID                              Hide SSID  Security Mode
-------  --------------------------------  ---------  -------------
1        ssid1                             Enable     Static WEP
2        dlink2                            Disable    None
3        dlink3                            Disable    None
4        dlink4                            Disable    None
5        dlink5                            Disable    None
6        dlink6                            Disable    None
7        dlink7                            Disable    None
8        dlink8                            Disable    None
9        dlink9                            Disable    None
10       dlink10                           Disable    None
11       dlink11                           Disable    None
12       dlink12                           Disable    None
13       dlink13                           Disable    None
14       dlink14                           Disable    None
15       dlink15                           Disable    None
16       dlink16                           Disable    None

Total Entries : 16

DWS-3160-24PC:admin#
```

To display a detailed view of a specific network:

```
DWS-3160-24PC:admin#show wireless network 1
Command: show wireless network 1

Network ID                                    : 1
SSID                                          : ssid1
Interface ID                                  : 7169
Default VLAN                                  : 2
Hide SSID                                     : Enable
Deny Broadcast                                : Enable
Redirect Mode                                 : HTTP
Redirect URL                                  : www.dlink.com
L2 Distributed Tunneling Mode                 : Enable
Bcast Key Refresh Rate                        : 1234
Session Key Refresh Rate                      : 2345
L3 Tunnel Mode                                : Enable
L3 Tunnel Status                              : Not Configured - No Routing
                                                Interface
L3 Tunnel Subnet IP                           : 20.20.0.0
L3 Tunnel Subnet Mask                         : 255.255.0.0
Wireless ARP Suppression                      : Disable
Security Mode                                 : Static WEP
MAC Authentication                            : RADIUS
RADIUS Use Network Configuration              : Enable
RADIUS Accounting                             : Enable
```

```
WPA Versions                                  : WPA2
WPA Ciphers                                   : TKIP
WPA Key Type                                  : ASCII
WPA Key                                       : wp4k3y12
WPA2 Pre-Authentication                       : Enable
WPA2 Pre-Authentication Limit                 : 120
WPA2 Key Caching Holdtime (minutes)           : 1200
WEP Authentication Type                       : Shared Key
WEP Key Type                                  : ASCII
WEP Key Length (bits)                         : 64
WEP Transfer Key Index                        : 2
WEP Key 1                                     : wk3y1
WEP Key 2                                     :
WEP Key 3                                     :
WEP Key 4                                     :
Client Qos Mode                               : Enable
Client QoS Bandwidth Limit Down(bps)          : 0
Client QoS Bandwidth Limit Up(bps)            : 11111
Client QoS Access Control Down                : IP - 1
Client QoS Access Control Up                  : IPv6 - ipv6acl
Client QoS Diffserv Policy Down               : qos_policy
Client QoS Diffserv Policy Up                 : -----

DWS-3160-24PC:admin#
```

Chapter 90 Wireless Peer Switch Command List

config wireless peer_switch [all | <ipaddr>]

config wireless peer_switch configuration [enable | disable] [all | ap_database | ap_profile | channelpower | discovery | global | known_client | radius_client | captive_portal | qos_acl | qos_diffserv]

show wireless configuration [request | receive]

show wireless peer_switch {<ipaddr> {[configure status | ap {<macaddr>}]}}

show wireless peer_switch ap {<macaddr>}

show wireless peer_switch configuration

show wireless peer_switch configure status

90-1 config wireless peer_switch

Description

This command is used to initiate a configuration push to one or all peer Switches.

Format

config wireless peer_switch [all | <ipaddr>]

Parameters

all - Specifies that a configuration will be pushed to all peer Switches.

<ipaddr> - Enter the IP address, of the specific Switch, that will receive the pushed configuration.

Restrictions

Only Administrators can issue this command.

Example

To initiate the configuration push for all peer Switches:

```
DWS-3160-24PC:admin#config wireless peer_switch all
Command: config wireless peer_switch all

Success.

DWS-3160-24PC:admin#
```

90-2 config wireless peer_switch configuration

Description

This command is used to enable or disable the peer Switch configuration for the wireless system. When a group is enabled, the corresponding configuration is applied to one or more peer Switches during a peer Switch configuration request.

Format

config wireless peer_switch configuration [enable | disable] [all | ap_database | ap_profile | channelpower | discovery | global | known_client | radius_client | captive_portal | qos_acl | qos_diffserv]

Parameters

enable - Specifies to enable the peer Switch configuration option for the wireless system.

disable - Specifies to disable the peer Switch configuration option for the wireless system.

all - Specifies to include all features listed below in the configuration that the Switch pushes to its peers.

ap_database - Specifies to include the AP Database in the configuration that the Switch pushes to its peers. By default, this option is enabled.

ap_profile - Specifies to include all AP profiles in the configuration that the Switch pushes to its peers. The AP profile includes the global AP settings, like the hardware type, radio settings, VAP and Wireless Network settings, and QoS settings. By default, this option is enabled.

channelpower - Specifies to include the RF management information in the configuration that the Switch pushes to its peers. By default, this option is enabled.

discovery - Specifies to include the Layer 2 and Layer 3 discovery information, including the VLAN list and IP list, in the configuration that the Switch pushes to its peers. Before pushing the IP discovery list from one Switch to another, make sure that the list contains IP addresses of all the Switches, including the Switch that is pushing the configuration. By default, this option is disabled.

global - Specifies to include basic and advanced global settings in the configuration that the Switch pushes to its peers. The configuration does not include the Switch IP address since that is a unique setting. By default, this option is enabled.

known_client - Specifies to include the Known Client Database in the configuration that the Switch pushes to its peers. By default, this option is enabled.

radius_client - Specifies to include client RADIUS information in the configuration that the Switch pushes to its peers. By default, this option is enabled.

captive_portal - Specifies to include Captive Portal information in the configuration that the Switch pushes to its peers. By default, this option is enabled.

qos_acl - Specifies to include the QoS ACLs in the configuration that the Switch pushes to its peers. By default, this option is enabled.

qos_diffserv - Specifies to include the Diffserv classes, services, and policies in the configuration that the Switch pushes to its peers. By default, this option is enabled.

Restrictions

Only Administrators can issue this command.

Example

To include all features in the configuration that the Switch pushes to its peers:

```
DWS-3160-24PC:admin#config wireless peer_switch configuration enable all
Command: config wireless peer_switch configuration enable all

Success.

DWS-3160-24PC:admin#
```

90-3 show wireless configuration

Description

This command is used to display the global peer Switch’s configuration push status and configuration push status for all peer Switches or the peer Switch’s configuration received status.

Format

show wireless configuration [request | receive]

Parameters

request - Specifies to display the configuration push status for all peer Switches.
receive - Specifies to display the peer Switch's configuration received status.

Restrictions

None.

Example

To display a wireless configuration request:

```
DWS-3160-24PC:admin#show wireless configuration request
Command: show wireless configuration request

Configuration Request Status                  : Complete
Total Count                                   : 1
Success Count                                 : 1
Failure Count                                 : 0

Peer IP Address       Configuration Request Status
-----------------     ------------------------------
192.168.69.124        Success

DWS-3160-24PC:admin#
```

To display a wireless configuration receive:

```
DWS-3160-24PC:admin#show wireless configuration receive
Command: show wireless configuration receive


Configuration Receive Status                : Not Started

Last Configuration Received
---------------------------
Peer Switch IP Address                        : 0.0.0.0
Configuration                                 : None
Timestamp                                     : -----

DWS-3160-24PC:admin#
```

In the above examples the following display parameters can be noticed:

Configuration Request Status - Displays the global status for the configuration push request.

Configuration Receive Status - Displays the status of the configuration push received from the peer switch.

Total Count - Displays the total number of peer switches configuration being pushed in the current configuration push request. This may be to one peer switch or to the total number of peer switches at the time the configuration push request is started.

Success Count - Displays the total number of peer switches to which the configuration has been pushed successfully for the current configuration push request.

Failure Count - Displays the total number of peer switches to which the configuration push request failed for the current configuration push request.

Peer IP Address - Displays the peer switch's IP address that pushed the configuration.

Configuration - Displays the configuration groups received as part of the configuration push.

Timestamp - Displays the configuration push received time.

90-4 show wireless peer_switch

Description

This command is used to displays status information for peer Wireless Switches.

Format

show wireless peer_switch {<ipaddr> {[configure status | ap {<macaddr>}]}}

Parameters

<ipaddr> - (Optional) Enter the IP address of a specific peer Switch here.

configure status - (Optional) Specifies to display the configuration push status information of peer wireless Switches.

ap - (Optional) Specifies to display the operational status of a peer Wireless Switch's managed AP. If no AP MAC address is specified, then the operational status for all APs is displayed. **<macaddr>** - Enter the peer Wireless Switch's managed AP MAC address used here.

Restrictions

None.

Example

To display the summary of status of all peer Switches:

```
DWS-3160-24PC:admin#show wireless peer_switch
Command: show wireless peer_switch

                  Vendor   Software              Protocol  Disc.
  IP Address      ID       Version               Version   Reason      Age
---------------  --------  --------------------  --------  ------- ------------
192.168.69.124   D-Link    4.0.0.1               2         IP Poll 0d:00:00:18

Total Entries : 1

DWS-3160-24PC:admin#
```

To display the detailed status of a specific peer Switch:

```
DWS-3160-24PC:admin#show wireless peer_switch 192.168.69.124
Command: show wireless peer_switch 192.168.69.124

IP Address                 : 192.168.69.124
Vendor ID                  : D-Link
Software Version           : 4.0.0.1
Protocol Version           : 2
Discovery Reason           : IP Poll
Managed AP Count           : 1
Age                        : 0d:00:00:38

DWS-3160-24PC:admin#
```

To display the detailed configuration push status of a specific peer Switch:

```
DWS-3160-24PC:admin#show wireless peer_switch 192.168.69.124 configure status
Command: show wireless peer_switch 192.168.69.124 configure status

IP Address                       : 192.168.69.124
Configuration Switch IP Address  : 192.168.69.123
Configuration                    : AP Database
                                   AP Profile
                                   Channel Power
                                   Global
                                   Known Client
                                   Captive Portal
                                   RADIUS Client
                                   QoS ACL
                                   QoS DiffServ
Timestamp                        : Sun Jan  2 01:59:36 GMT 2000

DWS-3160-24PC:admin#
```

To display a summary of all wireless Switch and managed APs:

```
DWS-3160-24PC:admin#show wireless peer_switch 192.168.69.124 ap
Command: show wireless peer_switch 192.168.69.124 ap

Peer Switch
MAC Address       IP Address      Location          Profile         HwType
----------------- --------------- ----------------- --------------- ---------
00-22-B0-3C-43-C0 192.168.69.124                    1-Default       hw_dwl8600

Total Entries : 1

DWS-3160-24PC:admin#
```

To display the detailed status of a specific AP:

```
DWS-3160-24PC:admin#show wireless peer_switch 192.168.69.124 ap 00-22-B0-3C-43-
C0
Command: show wireless peer_switch 192.168.69.124 ap 00-22-B0-3C-43-C0

MAC address                                   : 00-22-B0-3C-43-C0
Peer Switch IP Address                        : 192.168.69.124
IP Address                                    : 192.168.69.125
IP Subnet Mask                                : 255.255.255.0
Location                                      :
Profile                                       : 1-Default
Hardware Type                                 : hw_dwl8600

DWS-3160-24PC:admin#
```

90-5 show wireless peer_switch ap

Description

This command is used to display the operational status of the peer Wireless Switch’s managed AP(s). If no parameter are specified, this command will display a summary of all the Wireless Switch’s managed APs. If an AP MAC address is specified, a detailed status is displayed.

Format

show wireless peer_switch ap {<macaddr>}

Parameters

<macaddr> - (Optional) Enter the Wireless Switch's managed AP MAC address here.

Restrictions

None.

Example

To display a summary of all the Wireless Switch’s managed APs:

```
DWS-3160-24PC:admin#show wireless peer_switch ap
Command: show wireless peer_switch ap

                  Peer Switch
MAC Address       IP Address      Location          Profile         HwType
----------------- --------------- ----------------- --------------- ---------
00-22-B0-3C-43-C0 192.168.69.124                    1-Default       hw_dwl8600

Total Entries : 1

DWS-3160-24PC:admin#
```

To display the detailed status of a specific AP:

```
DWS-3160-24PC:admin#show wireless peer_switch ap 00-22-B0-3C-43-C0
Command: show wireless peer_switch ap 00-22-B0-3C-43-C0

MAC address                                   : 00-22-B0-3C-43-C0
Peer Switch IP Address                        : 192.168.69.124
IP Address                                    : 192.168.69.125
IP Subnet Mask                                : 255.255.255.0
Location                                      :
Profile                                       : 1-Default
Hardware Type                                 : hw_dwl8600

DWS-3160-24PC:admin#
```

90-6 show wireless peer_switch configuration

Description

This show command is used to display the peer Switch’s group configuration mode.

Format

show wireless peer_switch configuration

Parameters

None.

Restrictions

None.

Example

To display the peer Switch’s group configuration mode:

```
DWS-3160-24PC:admin#show wireless peer_switch configuration
Command: show wireless peer_switch configuration

AP Database           : Enabled
AP Profile            : Enabled
Channel Power         : Enabled
Discovery             : Enabled
Global                : Enabled
Known Client          : Enabled
Captive Portal        : Enabled
RADIUS Client         : Enabled
QoS ACL               : Enabled
QoS DiffServ          : Enabled

DWS-3160-24PC:admin#
```

90-7 show wireless peer_switch configure status

Description

This command is used to display the configuration push status information for peer wireless Switches.

Format

show wireless peer_switch configure status

Parameters

None.

Restrictions

None.

Example

To display the status of the peer Switch’s configuration push:

```
DWS-3160-24PC:admin#show wireless peer_switch configure status
Command: show wireless peer_switch configure status

                 Configuration      Configuration
Peer IP Address  Switch IP Address  Status            Timestamp
---------------  -----------------  ------------  ---------------------------
192.168.69.124   192.168.69.123     Success       Sun Jan  2 01:59:36 GMT 2000

Total Entries : 1

DWS-3160-24PC:admin#
```

In the above examples the following display parameters can be noticed:

Peer IP Address - Displays the IP address of the peer switch.

Configuration Switch IP Address - Displays the peer switch IP address last config received.

Configuration Status - Displays the configuration push status from the Wireless Switch to this peer switch.

Timestamp - Displays the time the config push was received from the peer switch.

Chapter 91 Wireless Provisioning and Mutual Authentication Command List

delete wireless ap_provisioning [<macaddr> | all]

config wireless ap_provision [<macaddr> [switch [primary | backup] <ipaddr> | profile [<int 1-16> | default] | start] | all start]

config wireless certificate_generate

config wireless certificate_request peer <ipaddr> start

config wireless cluster exchange_certificate

config wireless mutual_authentication_mode [enable | disable]

config wireless re_provisioning_unmanaged [enable | disable]

config wireless switch_provisioning [[enable | disable] | peer <ipaddr> start]

show wireless ap_provisioning {<macaddr>}

show wireless certificate_request

show wireless switch_provisioning

91-1 delete wireless ap_provisioning

Description

This command is used to remove the specified AP from the AP provisioning list or removes all APs from the AP provisioning list.

Format

delete wireless ap_provisioning [<macaddr> | all]

Parameters

<macaddr> - Enter the MAC Address of the AP here.

all - Specifies that all the APs will be removed from the AP provisioning list.

Restrictions

Only Administrators can issue this command.

Example

To delete a specified AP from the provisioning list:

```
DWS-3160-24PC:admin#delete wireless ap_provisioning 00-22-B0-3C-43-C0
Command: delete wireless ap_provisioning 00-22-B0-3C-43-C0

Success.

DWS-3160-24PC:admin#
```

To delete all entries from the provisioning list:

```
DWS-3160-24PC:admin#delete wireless ap_provisioning all
Command: delete wireless ap_provisioning all

Success.

DWS-3160-24PC:admin#
```

91-2 config wireless ap_provision

Description

This command is used to configure the AP provisioning settings.

Format

config wireless ap_provision [<macaddr> [switch [primary | backup] <ipaddr> | profile [<int 1-16> | default] | start] | all start]

Parameters

<macaddr> - Enter the MAC address of the AP here.

switch - Specifies that either a primary or backup Switch will be selected.
primary - Specifies the IP address of the primary Switch.
backup - Specifies the IP address of the backup Switch.

<ipaddr> - Enter the IP address of the primary or backup Switch, used, here.

profile - Specifies the profile ID used when provisioning of the AP takes place.
<int 1-16> - Enter the profile ID used here. This value must be between 1 and 16. The default value is 1.
default - Specifies that the default value will be used.

start - Specifies to initiate provisioning of the specified MAC address.

all start - Specifies to initiates provisioning of all the entries present in the AP provisioning database.

Restrictions

Only Administrators can issue this command.

Example

To configure the primary Switch for a specified AP:

```
DWS-3160-24PC:admin#config wireless ap_provision 00-22-B0-3C-43-C0 switch
primary 192.168.69.123
Command: config wireless ap_provision 00-22-B0-3C-43-C0 switch primary
192.168.69.123

Success.

DWS-3160-24PC:admin#
```

To configure the backup Switch for a specified AP:

```
DWS-3160-24PC:admin#config wireless ap_provision 00-22-B0-3C-43-C0 switch
backup 192.168.69.124
Command: config wireless ap_provision 00-22-B0-3C-43-C0 switch backup
192.168.69.124

Success.

DWS-3160-24PC:admin#
```

To configure the AP profile for a specified AP:

```
DWS-3160-24PC:admin#config wireless ap_provision 00-22-B0-3C-43-C0 profile 1
Command: config wireless ap_provision 00-22-B0-3C-43-C0 profile 1

Success.

DWS-3160-24PC:admin#
```

To configure the default profile for a specified AP:

```
DWS-3160-24PC:admin#config wireless ap_provision 00-22-B0-3C-43-C0 profile
default
Command: config wireless ap_provision 00-22-B0-3C-43-C0 profile default

Success.

DWS-3160-24PC:admin#
```

To initiate the provisioning of the specified MAC address in the AP Provisioning database:

```
DWS-3160-24PC:admin#config wireless ap_provision 00-22-B0-3C-43-C0 start
Command: config wireless ap_provision 00-22-B0-3C-43-C0 start

Success.

DWS-3160-24PC:admin#
```

To initiate the provisioning of all the entries present in the AP Provisioning database:

```
DWS-3160-24PC:admin#config wireless ap_provision all start
Command: config wireless ap_provision all start

Success.

DWS-3160-24PC:admin#
```

91-3 config wireless certificate_generate

Description

This command is used to initiate the regeneration of the X.509 certificate and RSA key on the wireless Switch.

Format

config wireless certificate_generate

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To initiate the regeneration of the X.509 certificate:

```
DWS-3160-24PC:admin#config wireless certificate_generate
Command: config wireless certificate_generate

Success.

DWS-3160-24PC:admin#
```

91-4 config wireless certificate_request peer

Description

This command is used to request a X.509 certificate from the cluster controller. The X.509 mutual certificate exchange is the only mechanism for peer Switches to authenticate with each other because Switches do not support a pass-phrase authentication. The X.509 certificate is automatically generated by the Switch and does not communicate with any trusted certificate authority.

Format

config wireless certificate_request peer <ipaddr> start

Parameters

<ipaddr> - Enter the IP address, of the wireless Switch, from which this Switch requests an X.509 certificate.

start - Specifies to start the request.

Restrictions

Only Administrators can issue this command.

Example

To start the wireless Switch certificate request:

```
DWS-3160-24PC:admin#config wireless certificate_request peer 192.168.69.123
start
Command: config wireless certificate_request peer 192.168.69.123 start

Success.

DWS-3160-24PC:admin#
```

91-5 config wireless cluster exchange_certificate

Description

This command is used to initiate trigger exchanges of X.509 certificates on the Switches and APs. This command can be triggered only when network mutual authentication is enabled.

Format

config wireless cluster exchange_certificate

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To initiate wireless cluster exchange certificates:

```
DWS-3160-24PC:admin#config wireless cluster exchange_certificate
Command: config wireless cluster exchange_certificate

Are you sure you want to trigger exchange of X.509 certificates in the cluster?
(y/n) y
 X.509 certificates exchange has been triggered.

Success.

DWS-3160-24PC:admin#
```

91-6 config wireless mutual_authentication_mode

Description

This command is used to configure the mutual authentication mode for the entire network or a cluster. This command causes the configuration to be updated and saved on all the Switches in the cluster. Switches and APs in the cluster will receive a X.509 certification used in mutual authentication. Mutual authentication provides security, when adding Switches and APs to the wireless network.

If Mutual authentication mode is enabled, the APs and Switches will perform the X.509 Mutual Certificate exchange. Each device compares the certificate received from the remote end-point with the local copy of the remote device's certificate. If the certificates don't match then the Transport Layer Security (TLS) connection is dropped.

Format

config wireless mutual_authentication_mode [enable | disable]

Parameters

enable - Specifies that mutual authentication will be enabled.
disable - Specifies that mutual authentication will be disabled.

Restrictions

Only Administrators can issue this command.

Example

To enable mutual authentication:

```
DWS-3160-24PC:admin# config wireless mutual_authentication_mode enable
Command: config wireless mutual_authentication_mode enable

Changing Mutual Authentication Mode might result in network traffic disruption.
Are you sure you want to continue? (y/n) y
 Network Mutual Authentication Mode set.

Success.

DWS-3160-24PC:admin#
```

To disable mutual authentication:

```
DWS-3160-24PC:admin#config wireless mutual_authentication_mode disable
Command: config wireless mutual_authentication_mode disable

Changing Mutual Authentication Mode might result in network traffic disruption.
Are you sure you want to continue? (y/n) y
 Network Mutual Authentication Mode set.

Success.

DWS-3160-24PC:admin#
```

91-7 config wireless re_provisioning_unmanaged

Description

The command is used to configure the re-provisioning of APs when its configure in the unmanaged mode. This configuration information is sent to all the Switches in the cluster and results in the saving of configurations on all the Switches in the network. This parameter is only applicable when mutual authentication is enabled.

The re-provisioning is allowed for unmanaged APs. This flag tells the AP whether it can accept provisioning information when it is not managed by a Switch. By default the AP can accept re-provisioning information. If the administrator disables re-provisioning in unmanaged mode then an AP cannot be managed by a Switch due to a certification mismatch. The administrator may need to factory reset the AP, which may require physical access to the AP. Note that in the case of a certification mismatch, disabling mutual authentication on the network won't allow the AP to join because the AP expects to be authenticated to the wireless switch. When the AP is in the managed mode, re-provisioning is always allowed. If mutual authentication is disabled on the AP then re-provisioning, in unmanaged mode, is always allowed.

Format

config wireless re_provisioning_unmanaged [enable | disable]

Parameters

enable - Specifies that the re-provisioning of APs, in the unmanaged mode, will be enabled. This is the default option.

disable - Specifies that the re-provisioning of APs, in the unmanaged mode, will be enabled.

Restrictions

Only Administrators can issue this command.

Example

To enable the unmanaged AP re-provisioning:

```
DWS-3160-24PC:admin#config wireless re_provisioning_unmanaged enable
Command: config wireless re_provisioning_unmanaged enable

This configuration will be sent to all switches in cluster.
Are you sure you want to continue? (y/n) y
 Unmanaged AP Re-provisioning Mode set.

Success.

DWS-3160-24PC:admin#
```

To disable the unmanaged AP re-provisioning:

```
DWS-3160-24PC:admin#config wireless re_provisioning_unmanaged disable
Command: config wireless re_provisioning_unmanaged disable

This configuration will be sent to all switches in cluster.
Are you sure you want to continue? (y/n) y
 Unmanaged AP Re-provisioning Mode set.

Success.

DWS-3160-24PC:admin#
```

91-8 config wireless switch_provisioning

Description

This command is used to configure Switch provisioning.

Format

config wireless switch_provisioning [[enable | disable] | peer <ipaddr> start]

Parameters

enable - Specifies that Switch provisioning will be enabled. This is the default option.
disable - Specifies that Switch provisioning will be disabled.

peer - Specifies the IP address of the Switch in a cluster, to which a new Switch establishes a connection to obtain provisioning information. The provisioning information enables the new Switch to join the cluster.
<ipaddr> - Enter the IP address of the Switch in a cluster here.

start - Specifies to start Switch provisioning.

Restrictions

Only Administrators can issue this command.

Example

To enabling Switch provisioning:

```
DWS-3160-24PC:admin#config wireless switch_provisioning enable
Command: config wireless switch_provisioning enable

Success.

DWS-3160-24PC:admin#
```

To start Switch provisioning:

```
DWS-3160-24PC:admin#config wireless switch_provisioning peer 192.168.69.123
start
Command: config wireless switch_provisioning peer 192.168.69.123 start

Success.

DWS-3160-24PC:admin#
```

91-9 show wireless ap_provisioning

Description

This command is used to display status information for entries in AP provisioning database. If no parameter is entered, the command displays a summary status for all entries in the database. If a client MAC address is entered, a detailed status for that entry is displayed.

Format

show wireless ap_provisioning {<macaddr>}

Parameters

<macaddr> - (Optional) Enter the Ethernet MAC address of the AP here.

Display parameters that can be found in the examples:

IP Address - Displays the IP address of the AP.

Primary Switch - Displays the IP address of the primary provisioned Switch as reported by the AP.

Backup Switch - Displays the IP address of the backup provisioned Switch as reported by the AP.

Mutual Authentication Mode - Displays the Mutual Authentication mode currently configured on the AP.

Unmanaged AP Re-provisioning Mode - Displays the re-provisioning mode currently configured on the AP.

New Primary Switch - Displays the IP address of the primary Switch with the Switch Administrator that wants to provision the AP.

New Backup Switch - Displays the IP address of the backup Switch with the Switch Administrator that wants to provision the AP.

New Profile ID - Displays the Profile ID configured in the local valid AP database of new primary and backup Switches.

AP Provisioning Status - Displays the status of the most recently issued AP provisioning command.

AP Certificate and Profile Transmit Status - Displasy the status of the last AP profile and certificate distribution to the primary and backup Switches.

Time Since Last Update - Displays the time since any information was received from this AP.

Restrictions

None.

Example

To display the status of all AP provisioning entries:

```
DWS-3160-24PC:admin#show wireless ap_provisioning
Command: show wireless ap_provisioning

 MAC Address       Primary          Backup          Provisioning   Time Since
 (*) Managed AP    Switch IP        Switch IP       Status         Last Update
------------------ --------------- --------------- -------------- ------------
 00-22-B0-3C-43-C0 192.168.69.123  192.168.69.124  Not Started    0d:00:00:02
*00-22-B0-3C-DD-C0 192.168.69.123  0.0.0.0         Unknown Failure0d:00:00:07

Total Entries : 2

DWS-3160-24PC:admin#
```

To display the status of a specified AP provisioning entry:

```
DWS-3160-24PC:admin#show wireless ap_provisioning 00-22-B0-3C-43-C0
Command: show wireless ap_provisioning 00-22-B0-3C-43-C0

MAC address                                   : 00-22-B0-3C-43-C0
AP IP Address                                 : 192.168.69.125
Primary Switch IP                             : 192.168.69.123
Backup Switch IP                              : 192.168.69.124
Mutual Authentication Mode                    : Disabled
Unmanaged AP Re-provisioning Mode            : Enabled
New Primary Switch IP                         : 0.0.0.0
New Backup Switch IP                          : 0.0.0.0
New Profile ID                                : 1 - Default
AP Provisioning Status                        : Not Started
AP Profile and Certificate Tx. Status         : Not Started
Time Since Last Update                        : 0d:00:00:05

DWS-3160-24PC:admin#
```

91-10 show wireless certificate_request

Description

This command is used to display the status of Switch certificate requests.

Format

show wireless certificate_request

Parameters

None.

Restrictions

None.

Example

To display the Switch’s certificate request status:

```
DWS-3160-24PC:admin#show wireless certificate_request
Command: show wireless certificate_request

Certificate Request Target IP Address         : 192.168.69.123
Certificate Request Status                    : Success

DWS-3160-24PC:admin#
```

91-11 show wireless switch_provisioning

Description

This command is used to display the Switch’s provisioning information.

Format

show wireless switch_provisioning

Parameters

None.

Restrictions

None.

Example

To display the Switch’s certificate request status:

```
DWS-3160-24PC:admin#show wireless switch_provisioning
Command: show wireless switch_provisioning

Provisioning Switch IP Address                : 192.168.69.123
Provisioning Status                           : Success

DWS-3160-24PC:admin#
```

Chapter 92 Wireless QoS Command List

create wireless access_list [mac <name 1-31> | ip [standard <int 1-99> | extended <int 100-199> | name <name 1-31>] | ipv6 <name 1-31>]

delete wireless access_list [mac <name 1-31> | ip [standard <int 1-99> | extended <int 100-199> | name <name 1-31>] | ipv6 <name 1-31>]

config wireless access_list ip extended <int 100-199> [add_rule <value 1-12> type [deny | permit] match_every [true | false {srcip <ipaddr> srcmask <netmask> | dstip <ipaddr> dstmask <netmask> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | service [ip_precedence <value 0-7> | ip_tos tos_bit <hex 0x00-0xff> tos_mask <hex 0x00-0xff> | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>]]}] | del_rule <value 1-12> | edit_rule <value 1-12> [type [deny | permit] | match_every [true | false] | srcip <ipaddr> srcmask <netmask> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | dstip <ipaddr> dstmask <netmask> | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | service [ip_precedence <value 0-7> | ip_tos tos_bit <hex 0x00-0xff> tos_mask <hex 0x00-0xff> | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 |be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>]]]]

config wireless access_list ip name <name 1-31> [rename <name 1-31> | add_rule <value 1-12> type [deny | permit] match_every [true | false {srcip <ipaddr> srcmask <netmask> | dstip <ipaddr> dstmask <netmask> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | service [ip_precedence <value 0-7> | ip_tos tos_bit <hex 0x00-0xff> tos_mask <hex 0x00-0xff> | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 |af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>]]}] | del_rule <value 1-12> | edit_rule <value 1-12> [type [deny | permit] | match_every [true | false] | srcip <ipaddr> srcmask <netmask> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | dstip <ipaddr> dstmask <netmask> | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | service [ip_precedence <value 0-7> | ip_tos tos_bit <hex 0x00-0xff> tos_mask <hex 0x00-0xff> | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>]]]]

config wireless access_list ip standard <int 1-99> [add_rule <value 1-12> type [deny | permit] match_every [true | false {srcip <ipaddr> srcmask <netmask>}] | del_rule <value 1-12> | edit_rule <value 1-12> [type [deny | permit] | match_every [true | false] | srcip <ipaddr> srcmask <netmask>]]

config wireless access_list ipv6 <name 1-31> [rename <name 1-31> | add_rule <value 1-10> type [deny | permit] match_every [true | false {src_ipv6 src_prefix <ipv6addr> src_prefix_length <int 1-128> | dst_ipv6 dst_prefix <ipv6addr> dst_prefix_length <int 1-128> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>] | flow_label <uint 0-1048575>}] | del_rule <value 1-10> | edit_rule <value 1-10> [type [deny | permit] | match_every [true | false] | src_prefix <ipv6addr> src_prefix_length <int 1-128> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | dst_prefix <ipv6addr> dst_prefix_length <int 1-128> | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 |

cs6 | cs7 | ef | other <int 0-63>] | flow_label <uint 0-1048575>]]

config wireless access_list mac <name 1-31> [rename <name 1-31> | add_rule <value 1-12> type [deny | permit] match_every [true | false {srcmac mac <macaddr> mask <macmask> | dstmac [mac <macaddr> mask <macmask> | bpdu] | ethertypekey [appletalk | arp | ibmsna | ipv4 | ipv6 | ipx | mplsmcast | mplsucast | netbios | rarp | user_value <hex 0x600-0xffff>] | cos <value 0-7> | vlan <vlanid 0-4095>}] | del_rule <value 1-12> | edit_rule <value 1-12> [type [deny | permit] | match_every [true | false] | srcmac mac <macaddr> mask <macmask> | dstmac mac <macaddr> mask <macmask> | ethertypekey [appletalk | arp | ibmsna | ipv4 | ipv6 | ipx | mplsmcast | mplsucast | netbios | rarp | user_value <hex 0x600-0xffff>] | cos <value 0-7> | vlan <vlanid0-4095>]]

create wireless diffserv class_map <name 1-31> match_all {[ipv4 | ipv6]}

delete wireless diffserv class_map <name 1-31>

create wireless diffserv policy_map <name 1-31>

delete wireless diffserv policy_map <name 1-31>

config wireless diffserv class_map <name 1-31> [rename <name 1-31> | match [ipv4 [any | cos <value 0-7> | dstmac <macaddr> mask <macmask> | dstip <ipaddr> dstmask <netmask> | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | ethertypekey [appletalk | arp | ibmsna | ipv4 | ipv6 | ipx | mplsmcast | mplsucast | netbios | rarp | user_value <hex 0x600-0xffff>] | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>] | ip_precedence <value 0-7> | ip_tos tos_bit <hex 0x00-0xff> tos_mask <hex 0x00-0xff> | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | reference_class <name 1-31> {remove} | srcmac <macaddr> mask <macmask> | srcip <ipaddr> srcmask <netmask> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | vlan <vlanid 0-4095>] | ipv6 [any | dstipv6 <ipv6addr> prefix_length <int 1-128> | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | flow_label <uint 0-1048575> | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>] | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | reference_class <name 1-31> {remove} | srcipv6 <ipv6addr> prefix_length <int 1-128> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>]]]]

config wireless diffserv policy_map <name 1-31> [rename <name 1-31> | add_class_member <name 1-31> | del_class_member <name 1-31> | class <name 1-31> action [drop | mark [cos <value 0-7> | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef] | ip_precedence <value 0-7>] | police_simple [color_blind committed_rate <uint 1-4294967295> committed_burst_size <int 1-128> conform_action [drop | set_prec_transmit <value 0-7> | set_dscp_transmit [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef] | set_cos_transmit <value 0-7> | send]]]]]

show wireless access_list [mac {<name 1-31>} | ip {[standard <int 1-99> | extended <int 100-199> | named <name 1-31>]} | ipv6 {<name 1-31>}]

show wireless diffserv {[class_map {class_name <name 1-31>} | policy_map {policy_name <name 1-31>}]}

92-1 create wireless access_list

Description

This command is used to create a MAC Access Control List (ACL), an IP ACL, an extended IP ACL, or an IPv6 ACL. The ACLs ensure that only authorized wireless users have access to specific resources and block any unwarranted attempts to reach wireless network resources.

Format

create wireless access_list [mac <name 1-31> | ip [standard <int 1-99> | extended <int 100-199> | name <name 1-31>] | ipv6 <name 1-31>]

Parameters

mac - Specifies to create a MAC ACL identified by its name.
  <name 1-31> - Enter the new MAC ACL name used here. This parameter is a case-sensitive alphanumeric field. This name can be up to 31 characters long.

ip - Specifies to create an IP ACL.
  standard - Specifies to create a standard IP ACL that is identified by the access list number.
    <int 1-99> - Enter the standard IP ACL access list number used here. This value must be between 1 and 99.
  extended - Specifies to create an extended IP ACL that is identified by the access list number.
    <int 100-199> - Enter the extended IP ACL access list number used here. This value must be between 100 and 199.
  name - Specifies to create an IP ACL that is identified by its name.
    <name 1-31> - Enter the new IP ACL name used here. This parameter is a case-sensitive alphanumeric field. This name can be up to 31 characters long.

ipv6 - Specifies to create an IPv6 ACL that is identified by its name.
  <name 1-31> - Enter the new IPv6 ACL name used here. This parameter is a case-sensitive alphanumeric field. This name can be up to 31 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create a MAC ACL:

```
DWS-3160-24PC:admin#create wireless access_list mac aclMac
Command: create wireless access_list mac aclMac

Success.

DWS-3160-24PC:admin#
```

To create a standard IP ACL:

```
DWS-3160-24PC:admin#create wireless access_list ip standard 5
Command: create wireless access_list ip standard 5

Success.

DWS-3160-24PC:admin#
```

92-2 delete wireless access_list

Description

This command is used to delete a MAC Access Control List (ACL), an IP ACL, an extended IP ACL, or an IPv6 ACL.

Format

delete wireless access_list [mac <name 1-31> | ip [standard <int 1-99> | extended <int 100-199> | name <name 1-31>] | ipv6 <name 1-31>]

Parameters

mac - Specifies to delete a MAC ACL identified by its name.
<name 1-31> - Enter the MAC ACL name used here. This parameter is a case-sensitive alphanumeric field. This name can be up to 31 characters long.

ip - Specifies to delete an IP ACL.
standard - Specifies to delete a standard IP ACL that is identified by the access list number.
<int 1-99> - Enter the standard IP ACL access list number used here. This value must be between 1 and 99.
extended - Specifies to delete an extended IP ACL that is identified by the access list number.
<int 100-199> - Enter the extended IP ACL access list number used here. This value must be between 100 and 199.
name - Specifies to delete an IP ACL that is identified by its name.
<name 1-31> - Enter the IP ACL name used here. This parameter is a case-sensitive alphanumeric field. This name can be up to 31 characters long.

ipv6 - Specifies to delete an IPv6 ACL that is identified by its name.
<name 1-31> - Enter the IPv6 ACL name used here. This parameter is a case-sensitive alphanumeric field. This name can be up to 31 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a MAC ACL:

```
DWS-3160-24PC:admin#delete wireless access_list mac aclMac
Command: delete wireless access_list mac aclMac

Success.

DWS-3160-24PC:admin#
```

To delete a standard IP ACL:

```
DWS-3160-24PC:admin#delete wireless access_list ip standard 5
Command: delete wireless access_list ip standard 5

Success.

DWS-3160-24PC:admin#
```

92-3 config wireless access_list ip extended

Description

This command is used to configure the related parameters of extended wireless access lists.

Format

config wireless access_list ip extended <int 100-199> [add_rule <value 1-12> type [deny | permit] match_every [true | false {srcip <ipaddr> srcmask <netmask> | dstip <ipaddr> dstmask <netmask> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | protocol [ip | icmp | igmp | tcp | udp | other <int

1-255>] | service [ip_precedence <value 0-7> | ip_tos tos_bit <hex 0x00-0xff> tos_mask <hex 0x00-0xff> | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>]]}] | del_rule <value 1-12> | edit_rule <value 1-12> [type [deny | permit] | match_every [true | false] | srcip <ipaddr> srcmask <netmask> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | dstip <ipaddr> dstmask <netmask> | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | service [ip_precedence <value 0-7> | ip_tos tos_bit <hex 0x00-0xff> tos_mask <hex 0x00-0xff> | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 |be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>]]]]

Parameters

extended - Specifies to configure a extended IP ACL, identified by ACL number.
- **<int 100-199>** - Enter the extended IP ACL number, used, here. This value must be between 100 and 199.
- **add_rule** - Specifies to create a new rule for a extended IP ACL.
  - **<value 1-12>** - Enter the new rule number for the new extended IP ACL here. This number must be between 1 and 12.
- **type** - Specifies what action should be taken if a packet matches the rule's criteria. The possible values are Permit or Deny.
  - **deny** - Specifies that the action, that will take place, if a packet matches the rule's criteria, is deny.
  - **permit** - Specifies that the action, that will take place, if a packet matches the rule's criteria, is permit.
- **match_every** - Specifies to match every packet. Valid values are true or false.
  - **true** - Specifies that every packet is considered to match the selected ACL Rule.
  - **false** - Specifies that it is not mandatory for every packet to match the selected ACL Rule.
- **srcip** - Specifies the source IP address of the IP ACL rule.
  - **<ipaddr>** - Enter the source IP address, of the IP ACL rule, here.
  - **srcmask** - Specifies the source netmask of the IP ACL rule.
    - **<netmask>** - Enter the source netmask, of the IP ACL rule, here.
- **dstip** - Specifies the destination IP address of the IP ACL rule.
  - **<ipaddr>** - Enter the destination IP address, of the IP ACL rule, here.
  - **dstmask** - Specifies the source netmask of the IP ACL rule.
    - **<netmask>** - Enter the destination netmask, of the IP ACL rule, here.
- **src_layer4_port** - Specifies the source Layer 4 port match condition for the IP ACL rule.
  - **domain** - Specifies that the source Layer 4 port match condition will use to port number of the service called Domain.
  - **echo** - Specifies that the source Layer 4 port match condition will use to port number of the service called Echo.
  - **ftp** - Specifies that the source Layer 4 port match condition will use to port number of the service called FTP.
  - **ftpdata** - Specifies that the source Layer 4 port match condition will use to port number of the service called FTP Data.
  - **http** - Specifies that the source Layer 4 port match condition will use to port number of the service called HTTP.
  - **smtp** - Specifies that the source Layer 4 port match condition will use to port number of the service called SMTP.
  - **snmp** - Specifies that the source Layer 4 port match condition will use to port number of the service called SNMP.
  - **telnet** - Specifies that the source Layer 4 port match condition will use to port number of the service called TELNET.
  - **tftp** - Specifies that the source Layer 4 port match condition will use to port number of the service called TFTP.
  - **other** - Specifies to use a custom port number that the source Layer 4 port match condition

will use.

<int 0-65535> - Enter the custom source Layer 4 port number used here. This value must be between 0 and 65535.

dst_layer4_port - Specifies the destination Layer 4 port match condition for the IP ACL rule.

domain - Specifies that the destination Layer 4 port match condition will use to port number of the service called Domain.

echo - Specifies that the destination Layer 4 port match condition will use to port number of the service called Echo.

ftp - Specifies that the destination Layer 4 port match condition will use to port number of the service called FTP.

ftpdata - Specifies that the destination Layer 4 port match condition will use to port number of the service called FTP Data.

http - Specifies that the destination Layer 4 port match condition will use to port number of the service called HTTP.

smtp - Specifies that the destination Layer 4 port match condition will use to port number of the service called SMTP.

snmp - Specifies that the destination Layer 4 port match condition will use to port number of the service called SNMP.

telnet - Specifies that the destination Layer 4 port match condition will use to port number of the service called TELNET.

tftp - Specifies that the destination Layer 4 port match condition will use to port number of the service called TFTP.

other - Specifies to use a custom port number that the destination Layer 4 port match condition will use.

<int 0-65535> - Enter the custom destination Layer 4 port number used here. This value must be between 0 and 65535.

protocol - Specifies the protocol to filter for an extended IP ACL rule, identified by number. The protocol number is a standard value assigned by IANA and is interpreted as an integer from 1 to 255. You can use the protocol number or you Specifies a protocol keyword.

ip - Specifies that the protocol, used to filter for an extended IP ACL rule, is IP.

icmp - Specifies that the protocol, used to filter for an extended IP ACL rule, is ICMP.

igmp - Specifies that the protocol, used to filter for an extended IP ACL rule, is IGMP.

tcp - Specifies that the protocol, used to filter for an extended IP ACL rule, is TCP.

udp - Specifies that the protocol, used to filter for an extended IP ACL rule, is UDP.

other - Specifies a custom protocol number to use in the extended IP ACL rule.

<int 1-255> - Enter the custom protocol number, used to filter for an extended IP ACL rule, here. This value must be between 1 and 255.

service - Specifies the Service Type match condition for the extended IP ACL rule.

ip_precedence - Specifies the IP precedence field in a packet that is defined as the high-order three bits of the Service Type octet in the IP header.

<value 0-7> - Enter the IP precedence value used here. This value must be between 0 and 7.

ip_tos - Specifies the IP ToS field in a packet that is defined as all eight bits of the Service Type octet in the IP header. The ToS Bits value is a two-digit hexadecimal number from 00 to ff. The TOS Mask value is a two-digit hexadecimal number from 0x00 to 0xff, representing an inverted mask. The zero-valued bits in the ToS Mask denote the bit positions in the ToS bits value that are used for comparison against the IP ToS field of a packet.

tos_bit - Specifies the ToS Bit value.

<hex 0x00-0xff> - Enter the ToS Bit value used here. This value must be between 0x00 and 0xff.

tos_mask - Specifies the ToS Mask value.

<hex 0x00-0xff> - Enter the ToS Mask value used here. This value must be between 0x00 and 0xff.

ip_dscp - Specifies the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order six bits of the Service Type octet in the IP header. The IP DSCP is configured by a possible selection of one of the DSCP keywords or a numerical values.

af11 - Specifies that the IP DiffServ Code Point value will be set as 'af11'.

af12 - Specifies that the IP DiffServ Code Point value will be set as 'af12'.

af13 - Specifies that the IP DiffServ Code Point value will be set as 'af13'.

af21 - Specifies that the IP DiffServ Code Point value will be set as 'af21'.
af22 - Specifies that the IP DiffServ Code Point value will be set as 'af22'.
af23 - Specifies that the IP DiffServ Code Point value will be set as 'af23'.
af31 - Specifies that the IP DiffServ Code Point value will be set as 'af31'.
af32 - Specifies that the IP DiffServ Code Point value will be set as 'af32'.
af33 - Specifies that the IP DiffServ Code Point value will be set as 'af33'.
af41 - Specifies that the IP DiffServ Code Point value will be set as 'af41'.
af42 - Specifies that the IP DiffServ Code Point value will be set as 'af42'.
af43 - Specifies that the IP DiffServ Code Point value will be set as 'af43'.
be - Specifies that the IP DiffServ Code Point value will be set as 'be'.
cs0 - Specifies that the IP DiffServ Code Point value will be set as 'cs0'.
cs1 - Specifies that the IP DiffServ Code Point value will be set as 'cs1'.
cs2 - Specifies that the IP DiffServ Code Point value will be set as 'cs2'.
cs3 - Specifies that the IP DiffServ Code Point value will be set as 'cs3'.
cs4 - Specifies that the IP DiffServ Code Point value will be set as 'cs4'.
cs5 - Specifies that the IP DiffServ Code Point value will be set as 'cs5'.
cs6 - Specifies that the IP DiffServ Code Point value will be set as 'cs6'.
cs7 - Specifies that the IP DiffServ Code Point value will be set as 'cs7'.
ef - Specifies that the IP DiffServ Code Point value will be set as 'ef'.
other - Specifies that a custom IP DiffServ Code Point value will be used.
<int 0-63> - Enter a custom IP DiffServ Code Point value here. This value must be between 0 and 63.

del_rule - Specifies to delete a specified rule from an extended IP ACL.
<value 1-12> - Enter the extended IP ACL number used here. This value must be between 1 and 12.

edit_rule - Specifies to update a specified rule from an extended IP ACL.
<value 1-12> - Enter the extended IP ACL number used here. This value must be between 1 and 12.

type - Specifies what action should be taken if a packet matches the rule's criteria. The possible values are Permit or Deny.
deny - Specifies that the action that will take place, if a packet matches the rule's criteria, is deny.
permit - Specifies that the action, that will take place, if a packet matches the rule's criteria, is permit.

match_every - Specifies to match every packet. Valid values are true or false.
true - Specifies that every packet is considered to match the selected ACL Rule.
false - Specifies that it is not mandatory for every packet to match the selected ACL Rule.

srcip - Specifies the source IP address of the IP ACL rule.
<ipaddr> - Enter the source IP address, of the IP ACL rule, here.
srcmask - Specifies the source netmask of the IP ACL rule.
<netmask> - Enter the source netmask, of the IP ACL rule, here.

src_layer4_port - Specifies the source Layer 4 port match condition for the IP ACL rule.
domain - Specifies that the source Layer 4 port match condition will use to port number of the service called Domain.
echo - Specifies that the source Layer 4 port match condition will use to port number of the service called Echo.
ftp - Specifies that the source Layer 4 port match condition will use to port number of the service called FTP.
ftpdata - Specifies that the source Layer 4 port match condition will use to port number of the service called FTP Data.
http - Specifies that the source Layer 4 port match condition will use to port number of the service called HTTP.
smtp - Specifies that the source Layer 4 port match condition will use to port number of the service called SMTP.
snmp - Specifies that the source Layer 4 port match condition will use to port number of the service called SNMP.
telnet - Specifies that the source Layer 4 port match condition will use to port number of the service called TELNET.
tftp - Specifies that the source Layer 4 port match condition will use to port number of the service called TFTP.

other - Specifies to use a custom port number that the source Layer 4 port match condition will use.

<int 0-65535> - Enter the custom source Layer 4 port number used here. This value must be between 0 and 65535.

dstip - Specifies the destination IP address of the IP ACL rule.

<ipaddr> - Enter the destination IP address, of the IP ACL rule, here.

dstmask - Specifies the source netmask of the IP ACL rule.

<netmask> - Enter the destination netmask, of the IP ACL rule, here.

dst_layer4_port - Specifies the destination Layer 4 port match condition for the IP ACL rule.

domain - Specifies that the destination Layer 4 port match condition will use to port number of the service called Domain.

echo - Specifies that the destination Layer 4 port match condition will use to port number of the service called Echo.

ftp - Specifies that the destination Layer 4 port match condition will use to port number of the service called FTP.

ftpdata - Specifies that the destination Layer 4 port match condition will use to port number of the service called FTP Data.

http - Specifies that the destination Layer 4 port match condition will use to port number of the service called HTTP.

smtp - Specifies that the destination Layer 4 port match condition will use to port number of the service called SMTP.

snmp - Specifies that the destination Layer 4 port match condition will use to port number of the service called SNMP.

telnet - Specifies that the destination Layer 4 port match condition will use to port number of the service called TELNET.

tftp - Specifies that the destination Layer 4 port match condition will use to port number of the service called TFTP.

other - Specifies to use a custom port number that the destination Layer 4 port match condition will use.

<int 0-65535> - Enter the custom destination Layer 4 port number used here. This value must be between 0 and 65535.

protocol - Specifies the protocol to filter for an extended IP ACL rule, identified by number. The protocol number is a standard value assigned by IANA and is interpreted as an integer from 1 to 255. You can use the protocol number or you Specifies a protocol keyword.

ip - Specifies that the protocol, used to filter for an extended IP ACL rule, is IP.

icmp - Specifies that the protocol, used to filter for an IP ACL rule, is ICMP.

igmp - Specifies that the protocol, used to filter for an IP ACL rule, is IGMP.

tcp - Specifies that the protocol, used to filter for an IP ACL rule, is TCP.

udp - Specifies that the protocol, used to filter for an IP ACL rule, is UDP.

other - Specifies a custom protocol number to use in the IP ACL rule.

<int 1-255> - Enter the custom protocol number, used to filter for an IP ACL rule, here. This value must be between 1 and 255.

service - Specifies the Service Type match condition for the IP ACL rule.

ip_precedence - Specifies the IP precedence field in a packet that is defined as the high-order three bits of the Service Type octet in the IP header.

<value 0-7> - Enter the IP precedence value used here. This value must be between 0 and 7.

ip_tos - Specifies the IP ToS field in a packet that is defined as all eight bits of the Service Type octet in the IP header. The ToS Bits value is a two-digit hexadecimal number from 00 to ff. The TOS Mask value is a two-digit hexadecimal number from 0x00 to 0xff, representing an inverted mask. The zero-valued bits in the ToS Mask denote the bit positions in the ToS bits value that are used for comparison against the IP ToS field of a packet.

tos_bit - Specifies the ToS Bit value.

<hex 0x00-0xff> - Enter the ToS Bit value used here. This value must be between 0x00 and 0xff.

tos_mask - Specifies the ToS Mask value.

<hex 0x00-0xff> - Enter the ToS Mask value used here. This value must be between 0x00 and 0xff.

ip_dscp - Specifies the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the

high-order six bits of the Service Type octet in the IP header. The IP DSCP is configured by a possible selection of one of the DSCP keywords or a numerical values.
af11 - Specifies that the IP DiffServ Code Point value will be set as 'af11'.
af12 - Specifies that the IP DiffServ Code Point value will be set as 'af12'.
af13 - Specifies that the IP DiffServ Code Point value will be set as 'af13'.
af21 - Specifies that the IP DiffServ Code Point value will be set as 'af21'.
af22 - Specifies that the IP DiffServ Code Point value will be set as 'af22'.
af23 - Specifies that the IP DiffServ Code Point value will be set as 'af23'.
af31 - Specifies that the IP DiffServ Code Point value will be set as 'af31'.
af32 - Specifies that the IP DiffServ Code Point value will be set as 'af32'.
af33 - Specifies that the IP DiffServ Code Point value will be set as 'af33'.
af41 - Specifies that the IP DiffServ Code Point value will be set as 'af41'.
af42 - Specifies that the IP DiffServ Code Point value will be set as 'af42'.
af43 - Specifies that the IP DiffServ Code Point value will be set as 'af43'.
be - Specifies that the IP DiffServ Code Point value will be set as 'be'.
cs0 - Specifies that the IP DiffServ Code Point value will be set as 'cs0'.
cs1 - Specifies that the IP DiffServ Code Point value will be set as 'cs1'.
cs2 - Specifies that the IP DiffServ Code Point value will be set as 'cs2'.
cs3 - Specifies that the IP DiffServ Code Point value will be set as 'cs3'.
cs4 - Specifies that the IP DiffServ Code Point value will be set as 'cs4'.
cs5 - Specifies that the IP DiffServ Code Point value will be set as 'cs5'.
cs6 - Specifies that the IP DiffServ Code Point value will be set as 'cs6'.
cs7 - Specifies that the IP DiffServ Code Point value will be set as 'cs7'.
ef - Specifies that the IP DiffServ Code Point value will be set as 'ef'.
other - Specifies that a custom IP DiffServ Code Point value will be used.
    <int 0-63> - Enter a custom IP DiffServ Code Point value here. This value must be between 0 and 63.

Restrictions

Only Administrators can issue this command.

Example

To create a new rule, for an existed IP extended ACL:

```
DWS-3160-24PC:admin#config wireless access_list ip extended 100 add_rule 1 type
permit match_every true
Command: config wireless access_list ip extended 100 add_rule 1 type permit
match_every true

Success.

DWS-3160-24PC:admin#config wireless access_list ip extended 100 add_rule 2 type
permit match_every false  src_layer4_port http protocol tcp
Command: config wireless access_list ip extended 100 add_rule 2 type permit
match_every false src_layer4_port http protocol tcp

Success.

DWS-3160-24PC:admin#
```

To update the protocol value of a specified rule of a IP extended ACL to be IGMP:

```
DWS-3160-24PC:admin#config wireless access_list ip extended 100 edit_rule 2
protocol igmp
Command: config wireless access_list ip extended 100 edit_rule 2 protocol igmp

Success.

DWS-3160-24PC:admin#
```

To delete a rule from an existed IP extended ACL:

```
DWS-3160-24PC:admin#config wireless access_list ip extended 100 del_rule 1
Command: config wireless access_list ip extended 100 del_rule 1

Success.

DWS-3160-24PC:admin#
```

92-4 config wireless access_list ip name

Description

This command is used to configure the related parameters of named wireless access lists.

Format

config wireless access_list ip name <name 1-31> [rename <name 1-31> | add_rule <value 1-12> type [deny | permit] match_every [true | false {srcip <ipaddr> srcmask <netmask> | dstip <ipaddr> dstmask <netmask> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | service [ip_precedence <value 0-7> | ip_tos tos_bit <hex 0x00-0xff> tos_mask <hex 0x00-0xff> | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 |af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>]]}] | del_rule <value 1-12> | edit_rule <value 1-12> [type [deny | permit] | match_every [true | false] | srcip <ipaddr> srcmask <netmask> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | dstip <ipaddr> dstmask <netmask> | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | service [ip_precedence <value 0-7> | ip_tos tos_bit <hex 0x00-0xff> tos_mask <hex 0x00-0xff> | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>]]]]

Parameters

named - Specifies to configure an IP ACL that is identified by name. This parameter uniquely identifies the IP access list.

<name 1-31> - Enter the named IP ACL name here. This name can be up to 31 characters long. This parameter is a case-sensitive alphanumeric string.

rename - Specifies to rename the currently specified named IP ACL.

<name 1-31> - Enter the named IP ACL name here. This name can be up to 31 characters long. This parameter is a case-sensitive alphanumeric string.

add_rule - Specifies to create a new rule for a named IP ACL.

<value 1-12> - Enter the new named IP ACL rule number here. This value must be between 1 and 12.

type - Specifies what action should be taken if a packet matches the rule's criteria. The possible values are Permit or Deny.
- **deny** - Specifies that the action that will take place, if a packet matches the rule's criteria, is deny.
- **permit** - Specifies that the action, that will take place, if a packet matches the rule's criteria, is permit.

match_every - Specifies to match every packet. Valid values are true or false.
- **true** - Specifies that every packet is considered to match the selected ACL Rule.
- **false** - Specifies that it is not mandatory for every packet to match the selected ACL Rule.

srcip - Specifies the source IP address of the IP ACL rule.
- **<ipaddr>** - Enter the source IP address, of the IP ACL rule, here.
- **srcmask** - Specifies the source netmask of the IP ACL rule.
  - **<netmask>** - Enter the source netmask, of the IP ACL rule, here.

dstip - Specifies the destination IP address of the IP ACL rule.
- **<ipaddr>** - Enter the destination IP address, of the IP ACL rule, here.
- **dstmask** - Specifies the source netmask of the IP ACL rule.
  - **<netmask>** - Enter the destination netmask, of the IP ACL rule, here.

src_layer4_port - Specifies the source Layer 4 port match condition for the IP ACL rule.
- **domain** - Specifies that the source Layer 4 port match condition will use to port number of the service called Domain.
- **echo** - Specifies that the source Layer 4 port match condition will use to port number of the service called Echo.
- **ftp** - Specifies that the source Layer 4 port match condition will use to port number of the service called FTP.
- **ftpdata** - Specifies that the source Layer 4 port match condition will use to port number of the service called FTP Data.
- **http** - Specifies that the source Layer 4 port match condition will use to port number of the service called HTTP.
- **smtp** - Specifies that the source Layer 4 port match condition will use to port number of the service called SMTP.
- **snmp** - Specifies that the source Layer 4 port match condition will use to port number of the service called SNMP.
- **telnet** - Specifies that the source Layer 4 port match condition will use to port number of the service called TELNET.
- **tftp** - Specifies that the source Layer 4 port match condition will use to port number of the service called TFTP.
- **other** - Specifies to use a custom port number that the source Layer 4 port match condition will use.
  - **<int 0-65535>** - Enter the custom source Layer 4 port number used here. This value must be between 0 and 65535.

dst_layer4_port - Specifies the destination Layer 4 port match condition for the IP ACL rule.
- **domain** - Specifies that the destination Layer 4 port match condition will use to port number of the service called Domain.
- **echo** - Specifies that the destination Layer 4 port match condition will use to port number of the service called Echo.
- **ftp** - Specifies that the destination Layer 4 port match condition will use to port number of the service called FTP.
- **ftpdata** - Specifies that the destination Layer 4 port match condition will use to port number of the service called FTP Data.
- **http** - Specifies that the destination Layer 4 port match condition will use to port number of the service called HTTP.
- **smtp** - Specifies that the destination Layer 4 port match condition will use to port number of the service called SMTP.
- **snmp** - Specifies that the destination Layer 4 port match condition will use to port number of the service called SNMP.
- **telnet** - Specifies that the destination Layer 4 port match condition will use to port number of the service called TELNET.
- **tftp** - Specifies that the destination Layer 4 port match condition will use to port number of the service called TFTP.
- **other** - Specifies to use a custom port number that the destination Layer 4 port match

condition will use.

<int 0-65535> - Enter the custom destination Layer 4 port number used here. This value must be between 0 and 65535.

protocol - Specifies the protocol to filter for a named IP ACL rule, identified by number. The protocol number is a standard value assigned by IANA and is interpreted as an integer from 1 to 255. You can use the protocol number or you Specifies a protocol keyword.

ip - Specifies that the protocol, used to filter for a named IP ACL rule, is IP.

icmp - Specifies that the protocol, used to filter for a named IP ACL rule, is ICMP.

igmp - Specifies that the protocol, used to filter for a named IP ACL rule, is IGMP.

tcp - Specifies that the protocol, used to filter for a named IP ACL rule, is TCP.

udp - Specifies that the protocol, used to filter for a named IP ACL rule, is UDP.

other - Specifies a custom protocol number to use in the named IP ACL rule.

<int 1-255> - Enter the custom protocol number, used to filter for a named IP ACL rule, here. This value must be between 1 and 255.

service - Specifies the Service Type match condition for the named IP ACL rule.

ip_precedence - Specifies the IP precedence field in a packet that is defined as the high-order three bits of the Service Type octet in the IP header.

<value 0-7> - Enter the IP precedence value used here. This value must be between 0 and 7.

ip_tos - Specifies the IP ToS field in a packet that is defined as all eight bits of the Service Type octet in the IP header. The ToS Bits value is a two-digit hexadecimal number from 00 to ff. The TOS Mask value is a two-digit hexadecimal number from 0x00 to 0xff, representing an inverted mask. The zero-valued bits in the ToS Mask denote the bit positions in the ToS bits value that are used for comparison against the IP ToS field of a packet.

tos_bit - Specifies the ToS Bit value.

<hex 0x00-0xff> - Enter the ToS Bit value used here. This value must be between 0x00 and 0xff.

tos_mask - Specifies the ToS Mask value.

<hex 0x00-0xff> - Enter the ToS Mask value used here. This value must be between 0x00 and 0xff.

ip_dscp - Specifies the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order six bits of the Service Type octet in the IP header. The IP DSCP is configured by a possible selection of one of the DSCP keywords or a numerical values.

af11 - Specifies that the IP DiffServ Code Point value will be set as 'af11'.

af12 - Specifies that the IP DiffServ Code Point value will be set as 'af12'.

af13 - Specifies that the IP DiffServ Code Point value will be set as 'af13'.

af21 - Specifies that the IP DiffServ Code Point value will be set as 'af21'.

af22 - Specifies that the IP DiffServ Code Point value will be set as 'af22'.

af23 - Specifies that the IP DiffServ Code Point value will be set as 'af23'.

af31 - Specifies that the IP DiffServ Code Point value will be set as 'af31'.

af32 - Specifies that the IP DiffServ Code Point value will be set as 'af32'.

af33 - Specifies that the IP DiffServ Code Point value will be set as 'af33'.

af41 - Specifies that the IP DiffServ Code Point value will be set as 'af41'.

af42 - Specifies that the IP DiffServ Code Point value will be set as 'af42'.

af43 - Specifies that the IP DiffServ Code Point value will be set as 'af43'.

be - Specifies that the IP DiffServ Code Point value will be set as 'be'.

cs0 - Specifies that the IP DiffServ Code Point value will be set as 'cs0'.

cs1 - Specifies that the IP DiffServ Code Point value will be set as 'cs1'.

cs2 - Specifies that the IP DiffServ Code Point value will be set as 'cs2'.

cs3 - Specifies that the IP DiffServ Code Point value will be set as 'cs3'.

cs4 - Specifies that the IP DiffServ Code Point value will be set as 'cs4'.

cs5 - Specifies that the IP DiffServ Code Point value will be set as 'cs5'.

cs6 - Specifies that the IP DiffServ Code Point value will be set as 'cs6'.

cs7 - Specifies that the IP DiffServ Code Point value will be set as 'cs7'.

ef - Specifies that the IP DiffServ Code Point value will be set as 'ef'.

other - Specifies that a custom IP DiffServ Code Point value will be used.

<int 0-63> - Enter a custom IP DiffServ Code Point value here. This value must be between 0 and 63.

del_rule - Specifies to delete a specified rule from a named IP ACL.

<value 1-12> - Enter the named IP ACL number used here. This value must be between 1 and 12.

edit_rule - Specifies to update a specified rule from a named IP ACL.

<value 1-12> - Enter the named IP ACL number used here. This value must be between 1 and 12.

type - Specifies what action should be taken if a packet matches the rule's criteria. The possible values are Permit or Deny.

deny - Specifies that the action that will take place, if a packet matches the rule's criteria, is deny.

permit - Specifies that the action, that will take place, if a packet matches the rule's criteria, is permit.

match_every - Specifies to match every packet. Valid values are true or false.

true - Specifies that every packet is considered to match the selected ACL Rule.

false - Specifies that it is not mandatory for every packet to match the selected ACL Rule.

srcip - Specifies the source IP address of the IP ACL rule.

<ipaddr> - Enter the source IP address, of the IP ACL rule, here.

srcmask - Specifies the source netmask of the IP ACL rule.

<netmask> - Enter the source netmask, of the IP ACL rule, here.

src_layer4_port - Specifies the source Layer 4 port match condition for the IP ACL rule.

domain - Specifies that the source Layer 4 port match condition will use to port number of the service called Domain.

echo - Specifies that the source Layer 4 port match condition will use to port number of the service called Echo.

ftp - Specifies that the source Layer 4 port match condition will use to port number of the service called FTP.

ftpdata - Specifies that the source Layer 4 port match condition will use to port number of the service called FTP Data.

http - Specifies that the source Layer 4 port match condition will use to port number of the service called HTTP.

smtp - Specifies that the source Layer 4 port match condition will use to port number of the service called SMTP.

snmp - Specifies that the source Layer 4 port match condition will use to port number of the service called SNMP.

telnet - Specifies that the source Layer 4 port match condition will use to port number of the service called TELNET.

tftp - Specifies that the source Layer 4 port match condition will use to port number of the service called TFTP.

other - Specifies to use a custom port number that the source Layer 4 port match condition will use.

<int 0-65535> - Enter the custom source Layer 4 port number used here. This value must be between 0 and 65535.

dstip - Specifies the destination IP address of the IP ACL rule.

<ipaddr> - Enter the destination IP address, of the IP ACL rule, here.

dstmask - Specifies the source netmask of the IP ACL rule.

<netmask> - Enter the destination netmask, of the IP ACL rule, here.

dst_layer4_port - Specifies the destination Layer 4 port match condition for the IP ACL rule.

domain - Specifies that the destination Layer 4 port match condition will use to port number of the service called Domain.

echo - Specifies that the destination Layer 4 port match condition will use to port number of the service called Echo.

ftp - Specifies that the destination Layer 4 port match condition will use to port number of the service called FTP.

ftpdata - Specifies that the destination Layer 4 port match condition will use to port number of the service called FTP Data.

http - Specifies that the destination Layer 4 port match condition will use to port number of the service called HTTP.

smtp - Specifies that the destination Layer 4 port match condition will use to port number of the service called SMTP.

snmp - Specifies that the destination Layer 4 port match condition will use to port number of the service called SNMP.

telnet - Specifies that the destination Layer 4 port match condition will use to port number of the service called TELNET.
tftp - Specifies that the destination Layer 4 port match condition will use to port number of the service called TFTP.
other - Specifies to use a custom port number that the destination Layer 4 port match condition will use.
<int 0-65535> - Enter the custom destination Layer 4 port number used here. This value must be between 0 and 65535.
protocol - Specifies the protocol to filter for an extended IP ACL rule, identified by number. The protocol number is a standard value assigned by IANA and is interpreted as an integer from 1 to 255. You can use the protocol number or you Specifies a protocol keyword.
ip - Specifies that the protocol, used to filter for an extended IP ACL rule, is IP.
icmp - Specifies that the protocol, used to filter for an IP ACL rule, is ICMP.
igmp - Specifies that the protocol, used to filter for an IP ACL rule, is IGMP.
tcp - Specifies that the protocol, used to filter for an IP ACL rule, is TCP.
udp - Specifies that the protocol, used to filter for an IP ACL rule, is UDP.
other - Specifies a custom protocol number to use in the IP ACL rule.
<int 1-255> - Enter the custom protocol number, used to filter for an IP ACL rule, here. This value must be between 1 and 255.
service - Specifies the Service Type match condition for the IP ACL rule.
ip_precedence - Specifies the IP precedence field in a packet that is defined as the high-order three bits of the Service Type octet in the IP header.
<value 0-7> - Enter the IP precedence value used here. This value must be between 0 and 7.
ip_tos - Specifies the IP ToS field in a packet that is defined as all eight bits of the Service Type octet in the IP header. The ToS Bits value is a two-digit hexadecimal number from 00 to ff. The TOS Mask value is a two-digit hexadecimal number from 0x00 to 0xff, representing an inverted mask. The zero-valued bits in the ToS Mask denote the bit positions in the ToS bits value that are used for comparison against the IP ToS field of a packet.
tos_bit - Specifies the ToS Bit value.
<hex 0x00-0xff> - Enter the ToS Bit value used here. This value must be between 0x00 and 0xff.
tos_mask - Specifies the ToS Mask value.
<hex 0x00-0xff> - Enter the ToS Mask value used here. This value must be between 0x00 and 0xff.
ip_dscp - Specifies the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order six bits of the Service Type octet in the IP header. The IP DSCP is configured by a possible selection of one of the DSCP keywords or a numerical values.
af11 - Specifies that the IP DiffServ Code Point value will be set as 'af11'.
af12 - Specifies that the IP DiffServ Code Point value will be set as 'af12'.
af13 - Specifies that the IP DiffServ Code Point value will be set as 'af13'.
af21 - Specifies that the IP DiffServ Code Point value will be set as 'af21'.
af22 - Specifies that the IP DiffServ Code Point value will be set as 'af22'.
af23 - Specifies that the IP DiffServ Code Point value will be set as 'af23'.
af31 - Specifies that the IP DiffServ Code Point value will be set as 'af31'.
af32 - Specifies that the IP DiffServ Code Point value will be set as 'af32'.
af33 - Specifies that the IP DiffServ Code Point value will be set as 'af33'.
af41 - Specifies that the IP DiffServ Code Point value will be set as 'af41'.
af42 - Specifies that the IP DiffServ Code Point value will be set as 'af42'.
af43 - Specifies that the IP DiffServ Code Point value will be set as 'af43'.
be - Specifies that the IP DiffServ Code Point value will be set as 'be'.
cs0 - Specifies that the IP DiffServ Code Point value will be set as 'cs0'.
cs1 - Specifies that the IP DiffServ Code Point value will be set as 'cs1'.
cs2 - Specifies that the IP DiffServ Code Point value will be set as 'cs2'.
cs3 - Specifies that the IP DiffServ Code Point value will be set as 'cs3'.
cs4 - Specifies that the IP DiffServ Code Point value will be set as 'cs4'.
cs5 - Specifies that the IP DiffServ Code Point value will be set as 'cs5'.
cs6 - Specifies that the IP DiffServ Code Point value will be set as 'cs6'.
cs7 - Specifies that the IP DiffServ Code Point value will be set as 'cs7'.

ef - Specifies that the IP DiffServ Code Point value will be set as 'ef'.
other - Specifies that a custom IP DiffServ Code Point value will be used.
<int 0-63> - Enter a custom IP DiffServ Code Point value here. This value must be between 0 and 63.

Restrictions

Only Administrators can issue this command.

Example

To create a new rule for an existed IP named ACL:

```
DWS-3160-24PC:admin#config wireless access_list ip name aclIPNamed-1 add_rule 1
type deny match_every true
Command: config wireless access_list ip name aclIPNamed-1 add_rule 1 type deny
match_every true

Success.

DWS-3160-24PC:admin#config wireless access_list ip name aclIPNamed-1 add_rule 2
type deny match_every false srcip 10.90.200.1 srcmask 255.255.255.0
dst_layer4_port ftp
Command: config wireless access_list ip name aclIPNamed-1 add_rule 2 type deny
match_every false srcip 10.90.200.1 srcmask 255.255.255.0 dst_layer4_port ftp

Success.

DWS-3160-24PC:admin#
```

To update the ‘match_every’ value of a specified rule of a IP named ACL to be false:

```
DWS-3160-24PC:admin# config wireless access_list ip name aclIPNamed-1 edit_rule
1 match_every false
Command: config wireless access_list ip name aclIPNamed-1 edit_rule 1
match_every false

Success.

DWS-3160-24PC:admin#
```

To delete a rule from an existed IP named ACL:

```
DWS-3160-24PC:admin#config wireless access_list ip name aclIPNamed-1 del_rule 1
Command: config wireless access_list ip name aclIPNamed-1 del_rule 1

Success.

DWS-3160-24PC:admin#
```

92-5 config wireless access_list ip standard

Description

This command is used to configure the related parameters of standard wireless access lists.

Format

config wireless access_list ip standard <int 1-99> [add_rule <value 1-12> type [deny | permit] match_every [true | false {srcip <ipaddr> srcmask <netmask>}] | del_rule <value 1-12> | edit_rule <value 1-12> [type [deny | permit] | match_every [true | false] | srcip <ipaddr> srcmask <netmask>]]

Parameters

standard - Specifies to configure a standard IP ACL, identified by the ACL number.
- **<int 1-99>** - Enter the standard IP ACL number, used, here. This value must be between 1 and 99.
- **add_rule** - Specifies to create a new rule for a standard IP ACL.
  - **<value 1-12>** - Enter the new rule number for the new standard IP ACL here. This number must be between 1 and 12.
- **type** - Specifies what action should be taken if a packet matches the rule's criteria. The possible values are Permit or Deny.
  - **deny** - Specifies that the action that will take place, if a packet matches the rule's criteria, is deny.
  - **permit** - Specifies that the action, that will take place, if a packet matches the rule's criteria, is permit.
- **match_every** - Specifies to match every packet. Valid values are true or false.
  - **true** - Specifies that every packet is considered to match the selected ACL Rule.
  - **false** - Specifies that it is not mandatory for every packet to match the selected ACL Rule.
- **srcip** - Specifies the source IP address of the IP ACL rule.
  - **<ipaddr>** - Enter the source IP address, of the IP ACL rule, here.
  - **srcmask** - Specifies the source netmask of the IP ACL rule.
    - **<netmask>** - Enter the source netmask, of the IP ACL rule, here.
- **del_rule** - Specifies to delete a specified rule from a standard IP ACL.
  - **<value 1-12>** - Enter the standard IP ACL number here. This value must be between 1 and 12.
- **edit_rule** - Specifies to update a specified rule of a standard IP ACL.
  - **<value 1-12>** - Enter the standard IP ACL number here. This value must be between 1 and 12.
- **type** - Specifies what action should be taken if a packet matches the rule's criteria. The possible values are Permit or Deny.
  - **deny** - Specifies that the action that will take place, if a packet matches the rule's criteria, is deny.
  - **permit** - Specifies that the action, that will take place, if a packet matches the rule's criteria, is permit.
- **match_every** - Specifies to match every packet. Valid values are true or false.
  - **true** - Specifies that every packet is considered to match the selected ACL Rule.
  - **false** - Specifies that it is not mandatory for every packet to match the selected ACL Rule.
- **srcip** - Specifies the source IP address of the IP ACL rule.
  - **<ipaddr>** - Enter the source IP address, of the IP ACL rule, here.
  - **srcmask** - Specifies the source netmask of the IP ACL rule.
    - **<netmask>** - Enter the source netmask, of the IP ACL rule, here.

Restrictions

Only Administrators can issue this command.

Example

To create a new rule, for an existed IP standard ACL:

```
DWS-3160-24PC:admin# config wireless access_list ip standard 5 add_rule 3 type
deny match_every false srcip 10.20.30.40 srcmask 255.0.0.0
Command: config wireless access_list ip standard 5 add_rule 1 type deny
match_every false srcip 10.20.30.40 srcmask 255.0.0.0


Success.


DWS-3160-24PC:admin#
```

To update the ‘match_every’ value of a specified rule of an standard IP ACL to be true:

```
DWS-3160-24PC:admin#config wireless access_list ip standard 5 edit_rule 3
match_every true
Command: config wireless access_list ip standard 5 edit_rule 3 match_every true


Success.


DWS-3160-24PC:admin#
```

To delete a rule from an existed IP standard ACL:

```
DWS-3160-24PC:admin#config wireless access_list ip standard 5 del_rule 3
Command: config wireless access_list ip standard 5 del_rule 1


Success.


DWS-3160-24PC:admin#
```

92-6 config wireless access_list ipv6

Description

This command is used to configure the related parameters of IPv6 wireless access lists.

Format

config wireless access_list ipv6 <name 1-31> [rename <name 1-31> | add_rule <value 1-10> type [deny | permit] match_every [true | false {src_ipv6 src_prefix <ipv6addr> src_prefix_length <int 1-128> | dst_ipv6 dst_prefix <ipv6addr> dst_prefix_length <int 1-128> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>] | flow_label <uint 0-1048575>}] | del_rule <value 1-10> | edit_rule <value 1-10> [type [deny | permit] | match_every [true | false] | src_prefix <ipv6addr> src_prefix_length <int 1-128> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | dst_prefix <ipv6addr> dst_prefix_length <int 1-128> | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>] | flow_label <uint 0-1048575>]]

Parameters

ipv6 - Specifies to configure an IPv6 ACL identified by name.

<name 1-31> - Enter the IPv6 ACL named used here. This name can be up to 31 characters long. This parameter is a case-sensitive alphanumeric string uniquely identifying the IPv6 access list.

rename - Specifies to rename the specified IPv6 ACL.

<name 1-31> - Enter the IPv6 ACL named used here. This name can be up to 31 characters long. This parameter is a case-sensitive alphanumeric string uniquely identifying the IPv6 access list.

add_rule - Specifies to create a new rule for an IPv6 ACL.

<value 1-10> - Enter the new rule number here. This value must be between 1 and 10.

type - Specifies what action should be taken if a packet matches the rule's criteria. The possible values are Permit or Deny.

deny - Specifies that the action that will take place, if a packet matches the rule's criteria, is deny.

permit - Specifies that the action, that will take place, if a packet matches the rule's criteria, is permit.

match_every - Specifies to match every packet. Valid values are true or false.

true - Specifies that every packet is considered to match the selected ACL Rule.

false - Specifies that it is not mandatory for every packet to match the selected ACL Rule.

src_ipv6 - Specifies the source IPv6 address of the IPv6 ACL rule.

src_prefix - Specifies the source IPv6 prefix of the IPv6 ACL rule.

<ipv6addr> - Enter the source IPv6 prefix value used here.

src_prefix_length - Specifies the source IPv6 prefix length of the IPv6 ACL rule.

<int 1-128> - Enter the source IPv6 prefix length of the IPv6 ACL rule here.

dst_ipv6 - Specifies the destination IPv6 address of the IPv6 ACL rule.

dst_prefix - Specifies the destination IPv6 prefix of the IPv6 ACL rule.

<ipv6addr> - Enter the destination IPv6 prefix value used here.

dst_prefix_length - Specifies the destination IPv6 prefix length of the IPv6 ACL rule.

<int 1-128> - Enter the destination IPv6 prefix length of the IPv6 ACL rule here.

src_layer4_port - Specifies the source Layer 4 port match condition for the IP ACL rule.

domain - Specifies that the source Layer 4 port match condition will use to port number of the service called Domain.

echo - Specifies that the source Layer 4 port match condition will use to port number of the service called Echo.

ftp - Specifies that the source Layer 4 port match condition will use to port number of the service called FTP.

ftpdata - Specifies that the source Layer 4 port match condition will use to port number of the service called FTP Data.

http - Specifies that the source Layer 4 port match condition will use to port number of the service called HTTP.

smtp - Specifies that the source Layer 4 port match condition will use to port number of the service called SMTP.

snmp - Specifies that the source Layer 4 port match condition will use to port number of the service called SNMP.

telnet - Specifies that the source Layer 4 port match condition will use to port number of the service called TELNET.

tftp - Specifies that the source Layer 4 port match condition will use to port number of the service called TFTP.

other - Specifies to use a custom port number that the source Layer 4 port match condition will use.

<int 0-65535> - Enter the custom source Layer 4 port number used here. This value must be between 0 and 65535.

dst_layer4_port - Specifies the destination Layer 4 port match condition for the IP ACL rule.

domain - Specifies that the destination Layer 4 port match condition will use to port number of the service called Domain.

echo - Specifies that the destination Layer 4 port match condition will use to port number of the service called Echo.

ftp - Specifies that the destination Layer 4 port match condition will use to port number of the service called FTP.

ftpdata - Specifies that the destination Layer 4 port match condition will use to port number of the service called FTP Data.

http - Specifies that the destination Layer 4 port match condition will use to port number of the service called HTTP.

smtp - Specifies that the destination Layer 4 port match condition will use to port number of the service called SMTP.

snmp - Specifies that the destination Layer 4 port match condition will use to port number of the service called SNMP.

telnet - Specifies that the destination Layer 4 port match condition will use to port number of the service called TELNET.

tftp - Specifies that the destination Layer 4 port match condition will use to port number of the service called TFTP.

other - Specifies to use a custom port number that the destination Layer 4 port match condition will use.

<int 0-65535> - Enter the custom destination Layer 4 port number used here. This value must be between 0 and 65535.

protocol - Specifies the protocol to filter for a named IPv6 ACL rule, identified by number. The protocol number is a standard value assigned by IANA and is interpreted as an integer from 1 to 255. You can use the protocol number or you Specifies a protocol keyword.

ip - Specifies that the protocol, used to filter for a named IPv6 ACL rule, is IP.

icmp - Specifies that the protocol, used to filter for a named IPv6 ACL rule, is ICMP.

igmp - Specifies that the protocol, used to filter for a named IPv6 ACL rule, is IGMP.

tcp - Specifies that the protocol, used to filter for a named IPv6 ACL rule, is TCP.

udp - Specifies that the protocol, used to filter for a named IPv6 ACL rule, is UDP.

other - Specifies a custom protocol number to use in the named IPv6 ACL rule.

<int 1-255> - Enter the custom protocol number, used to filter for a named IPv6 ACL rule, here. This value must be between 1 and 255.

ip_dscp - Specifies the IPv6 DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order six bits of the Service Type octet in the IPv6 header. The IPv6 DSCP is configured by a possible selection of one of the DSCP keywords or a numerical values.

af11 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af11'.

af12 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af12'.

af13 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af13'.

af21 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af21'.

af22 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af22'.

af23 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af23'.

af31 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af31'.

af32 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af32'.

af33 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af33'.

af41 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af41'.

af42 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af42'.

af43 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af43'.

be - Specifies that the IPv6 DiffServ Code Point value will be set as 'be'.

cs0 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs0'.

cs1 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs1'.

cs2 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs2'.

cs3 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs3'.

cs4 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs4'.

cs5 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs5'.

cs6 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs6'.

cs7 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs7'.

ef - Specifies that the IPv6 DiffServ Code Point value will be set as 'ef'.

other - Specifies that a custom IPv6 DiffServ Code Point value will be used.

<int 0-63> - Enter a custom IPv6 DiffServ Code Point value here. This value must be between 0 and 63.

flow_label - Specifies the value specified for IPv6 Flow Label.

<uint 0-1048575> - Enter the IPv6 Flow Label value here. This value must be between 0 and 1048575.

del_rule - Specifies to delete a specified rule from a named IPv6 ACL.

<value 1-10> - Enter the named IPv6 ACL number used here. This value must be between 1 and 10.

edit_rule - Specifies to update a specified rule from a named IPv6 ACL.

<value 1-10> - Enter the named IPv6 ACL number used here. This value must be between 1 and 10.

type - Specifies what action should be taken if a packet matches the rule's criteria. The possible values are Permit or Deny.

deny - Specifies that the action that will take place, if a packet matches the rule's criteria, is deny.

permit - Specifies that the action, that will take place, if a packet matches the rule's criteria, is permit.

match_every - Specifies to match every packet. Valid values are true or false.

true - Specifies that every packet is considered to match the selected ACL Rule.

false - Specifies that it is not mandatory for every packet to match the selected ACL Rule.

src_prefix - Specifies the source IPv6 prefix of the IPv6 ACL rule.

<ipv6addr> - Enter the source IPv6 prefix value used here.

src_prefix_length - Specifies the source IPv6 prefix length of the IPv6 ACL rule.

<int 1-128> - Enter the source IPv6 prefix length of the IPv6 ACL rule here.

src_layer4_port - Specifies the source Layer 4 port match condition for the IP ACL rule.

domain - Specifies that the source Layer 4 port match condition will use to port number of the service called Domain.

echo - Specifies that the source Layer 4 port match condition will use to port number of the service called Echo.

ftp - Specifies that the source Layer 4 port match condition will use to port number of the service called FTP.

ftpdata - Specifies that the source Layer 4 port match condition will use to port number of the service called FTP Data.

http - Specifies that the source Layer 4 port match condition will use to port number of the service called HTTP.

smtp - Specifies that the source Layer 4 port match condition will use to port number of the service called SMTP.

snmp - Specifies that the source Layer 4 port match condition will use to port number of the service called SNMP.

telnet - Specifies that the source Layer 4 port match condition will use to port number of the service called TELNET.

tftp - Specifies that the source Layer 4 port match condition will use to port number of the service called TFTP.

other - Specifies to use a custom port number that the source Layer 4 port match condition will use.

<int 0-65535> - Enter the custom source Layer 4 port number used here. This value must be between 0 and 65535.

dst_prefix - Specifies the destination IPv6 prefix of the IPv6 ACL rule.

<ipv6addr> - Enter the destination IPv6 prefix value used here.

dst_prefix_length - Specifies the destination IPv6 prefix length of the IPv6 ACL rule.

<int 1-128> - Enter the destination IPv6 prefix length of the IPv6 ACL rule here.

dst_layer4_port - Specifies the destination Layer 4 port match condition for the IP ACL rule.

domain - Specifies that the destination Layer 4 port match condition will use to port number of the service called Domain.

echo - Specifies that the destination Layer 4 port match condition will use to port number of the service called Echo.

ftp - Specifies that the destination Layer 4 port match condition will use to port number of the service called FTP.

ftpdata - Specifies that the destination Layer 4 port match condition will use to port number of the service called FTP Data.

http - Specifies that the destination Layer 4 port match condition will use to port number of the service called HTTP.

smtp - Specifies that the destination Layer 4 port match condition will use to port number of the service called SMTP.

snmp - Specifies that the destination Layer 4 port match condition will use to port number of the service called SNMP.

telnet - Specifies that the destination Layer 4 port match condition will use to port number of the service called TELNET.
tftp - Specifies that the destination Layer 4 port match condition will use to port number of the service called TFTP.
other - Specifies to use a custom port number that the destination Layer 4 port match condition will use.
<int 0-65535> - Enter the custom destination Layer 4 port number used here. This value must be between 0 and 65535.
protocol - Specifies the protocol to filter for a named IPv6 ACL rule, identified by number. The protocol number is a standard value assigned by IANA and is interpreted as an integer from 1 to 255. You can use the protocol number or you Specifies a protocol keyword.
ip - Specifies that the protocol, used to filter for a named IPv6 ACL rule, is IP.
icmp - Specifies that the protocol, used to filter for a named IPv6 ACL rule, is ICMP.
igmp - Specifies that the protocol, used to filter for a named IPv6 ACL rule, is IGMP.
tcp - Specifies that the protocol, used to filter for a named IPv6 ACL rule, is TCP.
udp - Specifies that the protocol, used to filter for a named IPv6 ACL rule, is UDP.
other - Specifies a custom protocol number to use in the named IPv6 ACL rule.
<int 1-255> - Enter the custom protocol number, used to filter for a named IPv6 ACL rule, here. This value must be between 1 and 255.
flow_label - Specifies the value specified for IPv6 Flow Label.
<uint 0-1048575> - Enter the IPv6 Flow Label value here. This value must be between 0 and 1048575.
ip_dscp - Specifies the IPv6 DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order six bits of the Service Type octet in the IPv6 header. The IPv6 DSCP is configured by a possible selection of one of the DSCP keywords or a numerical values.
af11 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af11'.
af12 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af12'.
af13 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af13'.
af21 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af21'.
af22 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af22'.
af23 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af23'.
af31 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af31'.
af32 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af32'.
af33 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af33'.
af41 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af41'.
af42 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af42'.
af43 - Specifies that the IPv6 DiffServ Code Point value will be set as 'af43'.
be - Specifies that the IPv6 DiffServ Code Point value will be set as 'be'.
cs0 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs0'.
cs1 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs1'.
cs2 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs2'.
cs3 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs3'.
cs4 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs4'.
cs5 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs5'.
cs6 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs6'.
cs7 - Specifies that the IPv6 DiffServ Code Point value will be set as 'cs7'.
ef - Specifies that the IPv6 DiffServ Code Point value will be set as 'ef'.
other - Specifies that a custom IPv6 DiffServ Code Point value will be used.
<int 0-63> - Enter a custom IPv6 DiffServ Code Point value here. This value must be between 0 and 63.
flow_label - Specifies the value specified for IPv6 Flow Label.
<uint 0-1048575> - Enter the IPv6 Flow Label value here. This value must be between 0 and 1048575.

Restrictions

Only Administrators can issue this command.

Example

To create a new rule for an existed IPv6 ACL:

```
DWS-3160-24PC:admin#config wireless access_list ipv6 aclIpv6-1 add_rule 1 type
deny match_every true
Command: config wireless access_list ipv6 aclIpv6-1 add_rule 1 type deny
match_every true

Success.

DWS-3160-24PC:admin#config wireless access_list ipv6 aclIpv6-1 add_rule 2 type
deny match_every false src_ipv6 src_prefix
2001:FECD:BA23:CD1F:DCB1:1010:9234:4088 src_prefix_length 22
Command: config wireless access_list ipv6 aclIpv6-1 add_rule 2 type deny
match_every false src_ipv6 src_prefix 2001:FECD:BA23:CD1F:DCB1:1010:9234:4088
src_prefix_length 22

Success.

DWS-3160-24PC:admin#
```

To update the ‘type’ value of a specified rule of an standard IPv6 ACL to be ‘permit’:

```
DWS-3160-24PC:admin# config wireless access_list ipv6 aclIpv6-1 edit_rule 1
type permit
Command: config wireless access_list ipv6 aclIpv6-1 edit_rule 1 type permit

Success.

DWS-3160-24PC:admin#
```

To delete a rule from an existed IPv6 ACL:

```
DWS-3160-24PC:admin#config wireless access_list ipv6 aclIpv6-1 del_rule 3
Command: config wireless access_list ipv6 aclIpv6-1 del_rule 3

Success.

DWS-3160-24PC:admin#
```

92-7 config wireless access_list mac

Description

This command is used to configure the related parameters of MAC wireless access lists.

Format

config wireless access_list mac <name 1-31> [rename <name 1-31> | add_rule <value 1-12> type [deny | permit] match_every [true | false {srcmac mac <macaddr> mask <macmask> | dstmac [mac <macaddr> mask <macmask> | bpdu] | ethertypekey [appletalk | arp | ibmsna | ipv4 | ipv6 | ipx | mplsmcast | mplsucast | netbios | rarp | user_value <hex 0x600-0xffff>] | cos <value 0-7> | vlan <vlanid 0-4095>}] | del_rule <value 1-12> | edit_rule <value 1-12> [type [deny | permit] | match_every [true | false] | srcmac mac <macaddr> mask <macmask> | dstmac mac <macaddr> mask <macmask> | ethertypekey [appletalk | arp | ibmsna | ipv4 |

ipv6 | ipx | mplsmcast | mplsucast | netbios | rarp | user_value <hex 0x600-0xffff>] | cos <value 0-7> | vlan <vlanid0-4095>]]

Parameters

mac - Specifies to configure a MAC ACL identified by name. The <name> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

<name 1-31> - Enter the MAC ACL name used here. This name can be up to 31 characters long.

rename - Specifies to rename the specified MAC ACL. The <name> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

<name 1-31> - Enter the MAC ACL name used here. This name can be up to 31 characters long.

add_rule - Specifies to create a new rule for a MAC ACL.

<value 1-12> - Enter the new rule, for a MAC ACL, value used here. This value must be between 1 and 12.

type - Specifies what action should be taken if a packet matches the rule's criteria. The possible values are Permit or Deny.

deny - Specifies to deny matching packets that fall within the rule's criteria.

permit - Specifies to permit matching packets that fall within the rule's criteria.

match_every - Specifies to match every Layer 2 MAC packet.

true - Specifies that every packet is considered to match the selected ACL Rule.

false - Specifies that it is not mandatory for every packet to match the selected ACL Rule.

srcmac - Specifies the source MAC address for this rule, to compare against an Ethernet frame.

mac - Specifies the source MAC address for this rule, to compare against an Ethernet frame.

<macaddr> - Enter the Source MAC address, for this rule, here.

mask - Specifies the source MAC address mask for this rule, indicating which bits in the source MAC to compare against an Ethernet frame.

<macmask> - Enter the source MAC address mask, for this rule, here.

dstmac - Specifies that the destination MAC address for this rule, will be configured.

mac - Specifies the destination MAC address for this rule, to compare against an Ethernet frame

<macaddr> - Enter the destination MAC address, for this rule, here.

mask - Specifies the destination MAC address mask for this rule, Specifiesing which bits in the destination MAC to compare against an Ethernet frame.

<macmask> - Enter the destination MAC address mask used here.

bpdu - Specifies the STP BPDU that is a Layer 2 packet and uses the multicast address of 01-80-C2-00-00-00 as the destination MAC and mask of FF-FF-FF-00-00-00.

ethertypekey - Specifies the Ethertype keyword or custom value for this rule and to compare against an Ethernet frame. The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. Each of these keywords translates into its equivalent Ethertype value(s).

appletalk - Specifies that the Ethertype keyword is 0x809B.

arp - Specifies that the Ethertype keyword is 0x0806.

ibmsna - Specifies that the Ethertype keyword is 0x80D5.

ipv4 - Specifies that the Ethertype keyword is 0x0800.

ipv6 - Specifies that the Ethertype keyword is 0x86DD.

ipx - Specifies that the Ethertype keyword is 0x8037.

mplsmcast - Specifies that the Ethertype keyword is 0x8848.

mplsucast - Specifies that the Ethertype keyword is 0x8847.

netbios - Specifies that the Ethertype keyword is 0x8191.

rarp - Specifies that the Ethertype keyword is 0x8035.

user_value - Specifies a custom user value for the Ethertype keyword.

<hex 0x600-0xffff> - Enter a user custom Ethertype keyword value here. This value must be between 0x600 and 0xffff.

cos - Specifies the CoS (802.1p user priority) value for this rule.

<value 0-7> - Enter the CoS value, for this rule, here. This value must be between 0 and 7.
vlan - Specifies the VLAN identifier value for this rule.
<vlanid 0-4095> - Enter the VLAN ID used here. This value must be between 0 and 4095.
del_rule - Specifies to delete a specified rule from a MAC ACL.
<value 1-12> - Enter the specific MAC ACL rule value, that will be deleted, here. This value must be between 1 and 12.
edit_rule - Specifies to update a specified rule of a MAC ACL.
<value 1-12> - Enter the specific MAC ACL rule value, that will be updated, here. This value must be between 1 and 12.
type - Specifies what action should be taken if a packet matches the rule's criteria. The possible values are Permit or Deny.
deny - Specifies that the action, that will be taken if a packet matches the rule's criteria, is deny.
permit - Specifies that the action, that will be taken if a packet matches the rule's criteria, is permit.
match_every - Specifies to match every Layer 2 MAC packet.
true - Specifies that every packet is considered to match the selected ACL Rule.
false - Specifies that it is not mandatory for every packet to match the selected ACL Rule.
srcmac - Specifies the source MAC address for this rule, to compare against an Ethernet frame.
mac - Specifies the source MAC address for this rule, to compare against an Ethernet frame.
<macaddr> - Enter the Source MAC address, for this rule, here.
mask - Specifies the source MAC address mask for this rule, indicating which bits in the source MAC to compare against an Ethernet frame.
<macmask> - Enter the source MAC address mask, for this rule, here.
dstmac - Specifies that the destination MAC address for this rule, will be configured.
mac - Specifies the destination MAC address for this rule, to compare against an Ethernet frame
<macaddr> - Enter the destination MAC address, for this rule, here.
mask - Specifies the destination MAC address mask for this rule, Specifiesing which bits in the destination MAC to compare against an Ethernet frame.
<macmask> - Enter the destination MAC address mask used here.
ethertypekey - Specifies the Ethertype keyword or custom value for this rule and to compare against an Ethernet frame. The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. Each of these keywords translates into its equivalent Ethertype value(s).
appletalk - Specifies that the Ethertype keyword is 0x809B.
arp - Specifies that the Ethertype keyword is 0x0806.
ibmsna - Specifies that the Ethertype keyword is 0x80D5.
ipv4 - Specifies that the Ethertype keyword is 0x0800.
ipv6 - Specifies that the Ethertype keyword is 0x86DD.
ipx - Specifies that the Ethertype keyword is 0x8037.
mplsmcast - Specifies that the Ethertype keyword is 0x8848.
mplsucast - Specifies that the Ethertype keyword is 0x8847.
netbios - Specifies that the Ethertype keyword is 0x8191.
rarp - Specifies that the Ethertype keyword is 0x8035.
user_value - Specifies a custom user value for the Ethertype keyword.
<hex 0x600-0xffff> - Enter a user custom Ethertype keyword value here. This value must be between 0x600 and 0xffff.
cos - Specifies the CoS (802.1p user priority) value for this rule.
<value 0-7> - Enter the CoS value, for this rule, here. This value must be between 0 and 7.
vlan - Specifies the VLAN identifier value for this rule.
<vlanid 0-4095> - Enter the VLAN ID used here. This value must be between 0 and 4095.

Restrictions

Only Administrators can issue this command.

Example

To create a new rule for an existed MAC ACL:

```
DWS-3160-24PC:admin#config wireless access_list mac aclMac add_rule 1 type
permit match_every true
Command: config wireless access_list mac aclMac add_rule 1 type permit
match_every true

Success.

DWS-3160-24PC:admin#config wireless access_list mac aclMac add_rule 2 type
permit match_every false dstmac mac 00-ED-12-BA-34-CF mask FF-FF-FF-FF-00-00
Command: config wireless access_list mac aclMac add_rule 2 type permit
match_every false dstmac mac 00-ED-12-BA-34-CF mask FF-FF-FF-FF-00-00

Success.

DWS-3160-24PC:admin#
```

To update the Ethertype value of a specified rule of a MAC ACL to be IPv6:

```
DWS-3160-24PC:admin#config wireless access_list mac aclMac edit_rule 2
ethertypekey ipv6
Command: config wireless access_list mac aclMac edit_rule 2 ethertypekey ipv6

Success.

DWS-3160-24PC:admin#
```

To delete a rule from an existed MAC ACL:

```
DWS-3160-24PC:admin# config wireless access_list mac aclMac del_rule 2
Command: config wireless access_list mac aclMac del_rule 2

Success.

DWS-3160-24PC:admin#
```

92-8 create wireless diffserv class_map

Description

This command is used to create a DiffServ class. Use the DiffServ class commands to define wireless traffic classification.

Format

create wireless diffserv class_map <name 1-31> match_all {[ipv4 | ipv6]}

Parameters

<name 1-31> - Enter the class map name used here. This name can be up to 31 characters long. This name is a case sensitive alphanumeric string that uniquely identifies a DiffServ class. The class map name “default” is reserved and must not be used.

match_all - Specifies the 'match all' class type and indicates that all of the individual match conditions must be true for a packet to be considered a member of the class.

- **ipv4** - (Optional) Specifies that the Layer 3 protocol used, for this class, is IPv4. This is the default option.
- **ipv6** - (Optional) Specifies that the Layer 3 protocol used, for this class, is IPv6.

Restrictions

Only Administrators can issue this command.

Example

To create a DiffServ class:

```
DWS-3160-24PC:admin#create wireless diffserv class_map cm1 match_all
Command: create wireless diffserv class_map cm1 match_all

Success.

DWS-3160-24PC:admin#create wireless diffserv class_map cm2 match_all ipv4
Command: create wireless diffserv class_map cm2 match_all ipv4

Success.

DWS-3160-24PC:admin#create wireless diffserv class_map cm3 match_all ipv6
Command: create wireless diffserv class_map cm3 match_all ipv6

Success.

DWS-3160-24PC:admin#
```

92-9 delete wireless diffserv class_map

Description

This command is used to delete an existing wireless DiffServ class.

Format

delete wireless diffserv class_map <name 1-31>

Parameters

<name 1-31> - Enter the class map name used here. This name can be up to 31 characters long. This name is a case sensitive alphanumeric string that uniquely identifies a DiffServ class. The class map name “default” is reserved and must not be used.

Restrictions

Only Administrators can issue this command.

Example

To delete an existing wireless Diffserv class used without any match condition:

```
DWS-3160-24PC:admin#delete wireless diffserv class_map cm1
Command: delete wireless diffserv class_map cm1

Success.

DWS-3160-24PC:admin#
```

To delete an existing wireless Diffserv class referenced by one or more policies:

```
DWS-3160-24PC:admin#delete wireless diffserv class_map cm3
Command: delete wireless diffserv class_map cm3

Error! Couldn't delete the Diffserv class.

Fail!

DWS-3160-24PC:admin#
```

92-10 create wireless diffserv policy_map

Description

This command is used to create a new DiffServ policy. Use the DiffServ policy commands to specify wireless traffic conditioning actions, such as policing and marking, to apply to traffic classes.

Format

create wireless diffserv policy_map <name 1-31>

Parameters

<name 1-31> - Enter the class map name used here. This name can be up to 31 characters long. This name is a case sensitive alphanumeric string that uniquely identifies a DiffServ class. The class map name “default” is reserved and must not be used.

Restrictions

Only Administrators can issue this command.

Example

To create a new DiffServ policy:

```
DWS-3160-24PC:admin#create wireless diffserv policy_map pm1
Command: create wireless diffserv policy_map pm1

Success.

DWS-3160-24PC:admin#
```

92-11 delete wireless diffserv policy_map

Description

This command is used to delete an existing wireless DiffServ policy.

Format

delete wireless diffserv policy_map <name 1-31>

Parameters

<name 1-31> - Enter the class map name used here. This name can be up to 31 characters long. This name is a case sensitive alphanumeric string that uniquely identifies a DiffServ class. The class map name “default” is reserved and must not be used.

Restrictions

Only Administrators can issue this command.

Example

To delete an existing wireless Diffserv policy:

```
DWS-3160-24PC:admin#delete wireless diffserv policy_map df_policy3
Command: delete wireless diffserv policy_map df_policy3

Success.

DWS-3160-24PC:admin#
```

92-12 config wireless diffserv class_map

Description

This command is used to configure the related parameters of a Class Map Wireless DiffServ.

Format

config wireless diffserv class_map <name 1-31> [rename <name 1-31> | match [ipv4 [any | cos <value 0-7> | dstmac <macaddr> mask <macmask> | dstip <ipaddr> dstmask <netmask> | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | ethertypekey [appletalk | arp | ibmsna | ipv4 | ipv6 | ipx | mplsmcast | mplsucast | netbios | rarp | user_value <hex 0x600-0xffff>] | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>] | ip_precedence <value 0-7> | ip_tos tos_bit <hex 0x00-0xff> tos_mask <hex 0x00-0xff> | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | reference_class <name 1-31> {remove} | srcmac <macaddr> mask <macmask> | srcip <ipaddr> srcmask <netmask> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | vlan <vlanid 0-4095>] | ipv6 [any | dstipv6 <ipv6addr> prefix_length <int 1-128> | dst_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>] | flow_label <uint 0-1048575> | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | other <int 0-63>] | protocol [ip | icmp | igmp | tcp | udp | other <int 1-255>] | reference_class <name 1-31> {remove} | srcipv6 <ipv6addr> prefix_length <int 1-

128> | src_layer4_port [domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | other <int 0-65535>]]]]

Parameters

class_map - Specifies the name of an existing wireless DiffServ class.
<name 1-31> - Enter the existing wireless DiffServ class name here. This name can be up to 31 characters long.
rename - Specifies to change the name of a wireless DiffServ class.
<name 1-31> - Enter the existing wireless DiffServ class name here. This name can be up to 31 characters long.
match - Specifies to configure a match criterion of a wireless DiffServ class.
ipv4 - Specifies that the Layer 3 protocol, for this class, is IPv4.
any - Specifies that all packets will be considered to belong to the class.
cos - Specifies the Class of Service value.
<value 0-7> - Enter the CoS value used here. This value must be between 0 and 7.
dstmac - Specifies the destination MAC address of a packet.
<macaddr> - Enter the destination MAC address of the packet here.
mask - Specifies the destination MAC mask of a packet.
<macmask> - Enter the destination MAC mask of the packet here.
dstip - Specifies the destination IP address of a packet.
<ipaddr> - Enter the destination IP address of the packet here.
dstmask - Specifies the destination IP mask of a packet.
<netmask> - Enter the destination IP mask of the packet here.
dst_layer4_port - Specifies the destination Layer 4 port of a packet, using a single keyword or numeric notation.
domain - Specifies that the destination Layer 4 port of a packet will use the service called Domain.
echo - Specifies that the destination Layer 4 port of a packet will use the service called Echo.
ftp - Specifies that the destination Layer 4 port of a packet will use the service called FTP.
ftpdata - Specifies that the destination Layer 4 port of a packet will use the service called FTP Data.
http - Specifies that the destination Layer 4 port of a packet will use the service called HTTP.
smtp - Specifies that the destination Layer 4 port of a packet will use the service called SMTP.
snmp - Specifies that the destination Layer 4 port of a packet will use the service called SNMP.
telnet - Specifies that the destination Layer 4 port of a packet will use the service called TELNET.
tftp - Specifies that the destination Layer 4 port of a packet will use the service called TFTP.
other - Specifies that a custom destination Layer 4 port number will be used.
<int 0-65535> - Enter the custom destination Layer 4 port number of a packet here. This value must be between 0 and 65535.
ethertypekey - Specifies the value of the Ethertype.
appletalk - Specifies that the Ethertype value will be configured as Apple Talk.
arp - Specifies that the Ethertype value will be configured as ARP.
ibmsna - Specifies that the Ethertype value will be configured as IBM Systems Network Architecture.
ipv4 - Specifies that the Ethertype value will be configured as IPv4.
ipv6 - Specifies that the Ethertype value will be configured as IPv6.
ipx - Specifies that the Ethertype value will be configured as IPX.
mplsmcast - Specifies that the Ethertype value will be configured as MPLS Multicast.
mplsuncast -Specifies that the Ethertype value will be configured as MPLS Unicast.
netbios - Specifies that the Ethertype value will be configured as NetBIOS.
rarp - Specifies that the Ethertype value will be configured as RARP.

user_value - Specifies that a custom Ethertype value will be used.
<0x0600-0xFFFF> - Enter the custom Ethertype value used here. This value must be between 0x0600 and 0xFFFF.
ip_dscp - Specifies the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header. The low-order two bits are not checked.
af11 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'af11'.
af12 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'af12'.
af13 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'af13'.
af21 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'af21'.
af22 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'af22'.
af23 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'af23'.
af31 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'af31'.
af32 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'af32'.
af33 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'af33'.
af41 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'af41'.
af42 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'af42'.
af43 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'af43'.
be - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'be'.
cs0 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'cs0'.
cs1 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'cs1'.
cs2 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'cs2'.
cs3 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'cs3'.
cs4 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'cs4'.
cs5 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'cs5'.
cs6 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'cs6'.
cs7 - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'cs7'.
ef - Specifies that the IP DiffServ Code Point (DSCP) field value will be set to 'ef'.
other - Specifies that a custom IP DiffServ Code Point (DSCP) field value will be used.
<int 0-63> - Enter the custom IP DiffServ Code Point (DSCP) field value here. This value must be between 0 and 63.
ip_precedence - Specifies the IP Precedence field value in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header. The low-order five bits are not checked.
<value 0-7> - Enter the IP Precedence field value used here. This value must be between 0 and 7.
ip_tos - Specifies the IP ToS field value in a packet, which is defined as all eight bits of the Service Type octet in the IP header.
tos_bit - Specifies the ToS Bit field value.
<hex 0x00-0xff> - Enter the ToS Bit field value here. This value must be between 0x00 and 0xff.
tos_mask - Specifies the ToS Mask field value.
<hex 0x00-0xff> - Enter the ToS Mask field value here. This value must be between 0x00 and 0xff.
protocol - Specifies the IP Protocol field value in a packet, using a single keyword notation or a numeric value notation.
ip - Specifies that the IP Protocol field value will be set as IP.
icmp - Specifies that the IP Protocol field value will be set as ICMP.
igmp - Specifies that the IP Protocol field value will be set as IGMP.
tcp - Specifies that the IP Protocol field value will be set as TCP.
udp - Specifies that the IP Protocol field value will be set as UDP.
other - Specifies to use a custom IP Protocol field value.
<int 1-255> - Enter the custom IP Protocol field value used here. This value must be between 1 and 255.
reference_class - Specifies the class reference name.
<name 1-31> - Enter the class reference name here. This name can be up to 31 characters long.
remove - (Optional) Specifies to remove the entry from the specified class definition when the set matches the conditions defined for another class.
srcmac - Specifies the source MAC address of a packet.

<macaddr> - Enter the source MAC address of a packet here.

mask - Specifies the source MAC mask of a packet.

<macmask> - Enter the source MAC mask of a packet here.

srcip - Specifies the source IP address of a packet.

<ipaddr> - Enter the source IP address of a packet here.

srcmask - Specifies the source IP mask of a packet.

<netmask> - Enter the source IP mask of a packet here.

src_layer4_port - Specifies the source Layer 4 port of a packet, using a single keyword or numeric notation.

domain - Specifies that the source Layer 4 port of a packet will use the service called Domain.

echo - Specifies that the source Layer 4 port of a packet will use the service called Echo.

ftp - Specifies that the source Layer 4 port of a packet will use the service called FTP.

ftpdata - Specifies that the source Layer 4 port of a packet will use the service called FTP Data.

http - Specifies that the source Layer 4 port of a packet will use the service called HTTP.

smtp - Specifies that the source Layer 4 port of a packet will use the service called SMTP.

snmp - Specifies that the source Layer 4 port of a packet will use the service called SNMP.

telnet - Specifies that the source Layer 4 port of a packet will use the service called TELNET.

tftp - Specifies that the source Layer 4 port of a packet will use the service called TFTP.

other - Specifies that a custom source Layer 4 port number will be used.

<int 0-65535> - Enter the custom source Layer 4 port number of a packet here. This value must be between 0 and 65535.

vlan - Specifies the Layer 2 VLAN Identifier field value (the only tag in a single tagged packet or the first or outer tag of a double VLAN tagged packet).

<vlanid 1-4095> - Enter the VLAN ID used here. This value must be between 1 and 4095.

ipv6 - Specifies that the Layer 3 protocol, for this class, is IPv6.

any - Specifies that all packets will be considered to belong to the class.

dstipv6 - Specifies the destination IPv6 address of a packet.

<ipv6addr> - Enter the destination IPv6 address of a packet here.

prefix_length - Specifies the destination IPv6 prefix length of a packet.

<int 1-128> - Enter the destination IPv6 prefix length of a packet here. This value must be between 1 and 128.

dst_layer4_port - Specifies the destination Layer 4 port of a packet, using a single keyword or numeric notation.

domain - Specifies that the destination Layer 4 port of a packet will use the service called Domain.

echo - Specifies that the destination Layer 4 port of a packet will use the service called Echo.

ftp - Specifies that the destination Layer 4 port of a packet will use the service called FTP.

ftpdata - Specifies that the destination Layer 4 port of a packet will use the service called FTP Data.

http - Specifies that the destination Layer 4 port of a packet will use the service called HTTP.

smtp - Specifies that the destination Layer 4 port of a packet will use the service called SMTP.

snmp - Specifies that the destination Layer 4 port of a packet will use the service called SNMP.

telnet - Specifies that the destination Layer 4 port of a packet will use the service called TELNET.

tftp - Specifies that the destination Layer 4 port of a packet will use the service called TFTP.

other - Specifies that a custom destination Layer 4 port number will be used.

<int 0-65535> - Enter the custom destination Layer 4 port number of a packet here. This value must be between 0 and 65535.

flow_label - Specifies the IPv6 Flow Label.

<uint 0-1048575> - Enter the IPv6 Flow Label used here. This value must be between 0 and 1048575.

ip_dscp - Specifies the value of the IPv6 DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IPv6 header. The low-order two bits are not checked.

af11 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'af11'.

af12 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'af12'.

af13 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'af13'.

af21 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'af21'.

af22 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'af22'.

af23 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'af23'.

af31 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'af31'.

af32 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'af32'.

af33 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'af33'.

af41 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'af41'.

af42 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'af42'.

af43 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'af43'.

be - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'be'.

cs0 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'cs0'.

cs1 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'cs1'.

cs2 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'cs2'.

cs3 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'cs3'.

cs4 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'cs4'.

cs5 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'cs5'.

cs6 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'cs6'.

cs7 - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'cs7'.

ef - Specifies that the IPv6 DiffServ Code Point (DSCP) field value will be set to 'ef'.

other - Specifies that a custom IPv6 DiffServ Code Point (DSCP) field value will be used.

<int 0-63> - Enter the custom IPv6 DiffServ Code Point (DSCP) field value here. This value must be between 0 and 63.

protocol - Specifies the IPv6 Protocol field value in a packet, using a single keyword notation or a numeric value notation.

ip - Specifies that the IPv6 Protocol field value will be set as IP.

icmp - Specifies that the IPv6 Protocol field value will be set as ICMP.

igmp - Specifies that the IPv6 Protocol field value will be set as IGMP.

tcp - Specifies that the IPv6 Protocol field value will be set as TCP.

udp - Specifies that the IPv6 Protocol field value will be set as UDP.

other - Specifies to use a custom IPv6 Protocol field value.

<int 1-255> - Enter the custom IPv6 Protocol field value used here. This value must be between 1 and 255.

reference_class - Specifies the class reference name.

<name 1-31> - Enter the class reference name here. This name can be up to 31 characters long.

remove - (Optional) Specifies to remove the entry from the specified class definition when the set matches the conditions defined for another class.

srcipv6 - Specifies the source IPv6 address of a packet.

<ipv6addr> - Enter the source IPv6 address of a packet here.

prefix_length - Specifies the source IPv6 prefix length of a packet.

<int 1-128> - Enter the source IPv6 prefix length of a packet here.

src_layer4_port - Specifies the source Layer 4 port of a packet, using a single keyword or numeric notation.

domain - Specifies that the source Layer 4 port of a packet will use the service called Domain.

echo - Specifies that the source Layer 4 port of a packet will use the service called Echo.

ftp - Specifies that the source Layer 4 port of a packet will use the service called FTP.

ftpdata - Specifies that the source Layer 4 port of a packet will use the service called FTP Data.

http - Specifies that the source Layer 4 port of a packet will use the service called HTTP.

smtp - Specifies that the source Layer 4 port of a packet will use the service called SMTP.

snmp - Specifies that the source Layer 4 port of a packet will use the service called SNMP.

telnet - Specifies that the source Layer 4 port of a packet will use the service called TELNET.

tftp - Specifies that the source Layer 4 port of a packet will use the service called TFTP.

other - Specifies that a custom source Layer 4 port number will be used.

<int 0-65535> - Enter the custom source Layer 4 port number of a packet here. This value must be between 0 and 65535.

Restrictions

Only Administrators can issue this command.

Example

To change the name of an existing wireless DiffServ class:

```
DWS-3160-24PC:admin#config wireless diffserv class_map cm50 rename cm30
Command: config wireless diffserv class_map cm50 rename cm30

Success.

DWS-3160-24PC:admin#
```

To configure a match criterion, source IP address, of an existing wireless DiffServ class:

```
DWS-3160-24PC:admin#config wireless diffserv class_map cm1 match ipv4 srcip
10.90.100.1 srcmask 255.0.0.0
Command: config wireless diffserv class_map cm1 match ipv4 srcip 10.90.100.1
srcmask 255.0.0.0

Success.

DWS-3160-24PC:admin#
```

92-13 config wireless diffserv policy_map

Description

This command is used to configure the related parameters of Policy Map Wireless DiffServ.

Format

config wireless diffserv policy_map <name 1-31> [rename <name 1-31> | add_class_member <name 1-31> | del_class_member <name 1-31> | class <name 1-31> action [drop | mark [cos <value 0-7> | ip_dscp [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef] | ip_precedence <value 0-7>] | police_simple [color_blind committed_rate <uint 1-4294967295> committed_burst_size <int 1-128> conform_action [drop | set_prec_transmit <value 0-7> | set_dscp_transmit [af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef] | set_cos_transmit <value 0-7> | send]]]]]

Parameters

policy_map - Specifies the name of an existing wireless DiffServ policy.

<name 1-31> - Enter the name of an existing wireless DiffServ policy here. This name can be up to 31 characters long.

rename - Specifies to change the name of an existing wireless DiffServ policy.

<name 1-31> - Enter the name of an existing wireless DiffServ policy here. This name can be up to 31 characters long.

add_class_member - Specifies to create an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements. This command causes the specified policy to create a reference to the class definition.

<name 1-31> - Enter the name of the class member here. This name can be up to 31 characters long.

del_class_member - Specifies to delete the instance of a particular class and its defined treatment from the specified policy. This command removes the reference to the class definition for the specified policy.

<name 1-31> - Enter the name of the class member here. This name can be up to 31 characters long.

class - Specifies the name of an existing wireless DiffServ class.

<name 1-31> - Enter the name of an existing wireless DiffServ class here.

action - Specifies the traffic conditioning actions, such as policing and marking, to apply to traffic classes.

drop - Specifies that all packets for the associated traffic stream are to be dropped at the ingress.

mark cos - Specifies to mark all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header. If the packet does not already contain this header, one is inserted.

<value 0-7> - Enter the CoS mark value used here. This value must be between 0 and 7.

ip_dscp - Specifies to mark all packets, of the associated traffic stream, with the specified IP DSCP value.

af11 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af11'.
af12 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af12'.
af13 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af13'.
af21 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af21'.
af22 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af22'.
af23 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af23'.
af31 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af31'.
af32 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af32'.

af33 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af33'.
af41 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af41'.
af42 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af42'.
af43 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af43'.
be - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'be'.
cs0 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs0'.
cs1 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs1'.
cs2 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs2'.
cs3 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs3'.
cs4 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs4'.
cs5 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs5'.
cs6 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs6'.
cs7 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs7'.
ef - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'ef'.

ip_precedence - Specifies to mark all packets, of the associated traffic stream, with the specified IP Precedence value. This command may not be used on IPv6 classes. IPv6 does not have a precedence field.

<value 0-7> - Enter the IP Precedence value used here. This value must be between 0 and 7.

police_simple - Specifies to establish the traffic policing style for the specified class. This command uses a single data rate and burst size resulting in an outcome called conform.

color_blind - Specifies that the color-blind method will be used.

committed_rate - Specifies that the committed rate is used to monitor the arrival rate of incoming packets for this class.

<uint 1-4294967295> - Enter the committed rate is used to monitor the arrival rate of incoming packets for this class here. This value must be between 1 and 4294967295 bits-per-second (bps).

committed_burst_size - Specifies the committed burst size used to determine the amount of conforming traffic allowed.

<int 1-128> - Enter the committed burst size used to determine the amount of conforming traffic allowed here. This value must be between 1 and 128 Kbytes.

conform_action drop - Specifies that packets are immediately dropped upon conforming that packets match the policing metrics.

set_prec_transmit - Specifies that packets are marked by DiffServ with the specified IP Precedence value before being presented to the system's forwarding element upon conforming that these packets match the policing metrics. This selection requires that the Mark IP Precedence value field be set.

<int 0-7> - Enter the IP Precedence transmit value here. This value must between 0 and 7.

set_dscp_transmit - Specifies that packets are marked by DiffServ with the specified DSCP value before being presented to the system's forwarding element upon conforming that packets match the policing metrics. This selection requires that the DSCP value field be set.

af11 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af11'.
af12 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af12'.
af13 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af13'.
af21 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af21'.
af22 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af22'.
af23 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af23'.
af31 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af31'.
af32 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af32'.
af33 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af33'.
af41 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af41'.
af42 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af42'.
af43 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'af43'.
be - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'be'.
cs0 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs0'.
cs1 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs1'.
cs2 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs2'.
cs3 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs3'.

cs4 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs4'.
cs5 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs5'.
cs6 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs6'.
cs7 - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'cs7'.
ef - Specifies that the DiffServ Code Point (DSCP) field value will be set to 'ef'.

set_cos_transmit - Specifies that packets are marked by DiffServ with the specified CoS value before being presented to the system's forwarding element upon conforming that packets match the policing metrics. This selection requires that the Mark CoS value field be set.

<int 0-7> - Enter the CoS transmit value used here. This value must be between 0 and 7.

send - Specifies that packets are presented unmodified by DiffServ to the system's forwarding element upon conforming that packets match the policing metrics.

Restrictions

Only Administrators can issue this command.

Example

To change the name of an existing wireless DiffServ policy:

```
DWS-3160-24PC:admin#config wireless diffserv policy_map df_policy1 rename 
df_policy2
Command: config wireless diffserv policy_map df_policy1 rename df_policy2

Success.

DWS-3160-24PC:admin#
```

To create a policy class instance by attaching the specified class to the policy:

```
DWS-3160-24PC:admin#config wireless diffserv policy_map df_policy1 
add_class_member cm30
Command: config wireless diffserv policy_map df_policy1 add_class_member cm30

Success.

DWS-3160-24PC:admin#
```

To remove a policy class instance by detaching the specified class from the policy:

```
DWS-3160-24PC:admin#config wireless diffserv policy_map df_policy1 
del_class_member cm30
Command: config wireless diffserv policy_map df_policy1 del_class_member cm30

Success.

DWS-3160-24PC:admin#
```

To configure a policy class instance to use the drop action:

```
DWS-3160-24PC:admin#config wireless diffserv policy_map df_policy class cm30
action drop
Command: config wireless diffserv policy_map df_policy class cm30 action drop

Success.

DWS-3160-24PC:admin#
```

92-14 show wireless access_list

Description

This command is used to display summary information of the wireless access list configuration for a specified ACL type or the detailed configuration of one specified wireless access list.

Format

show wireless access_list [mac {<name 1-31>} | ip {[standard <int 1-99> | extended <int 100-199> | named <name 1-31>]} | ipv6 {<name 1-31>}]

Parameters

mac - Specifies to display a MAC ACL identified by its name.

- **<name 1-31>** - (Optional) Enter the MAC ACL name used here. This parameter is a case-sensitive alphanumeric field. This name can be up to 31 characters long.

ip - Specifies to display an IP ACL.

- **standard** - (Optional) Specifies to display a standard IP ACL that is identified by the access list number.
  - **<int 1-99>** - Enter the standard IP ACL access list number used here. This value must be between 1 and 99.
- **extended** - (Optional) Specifies to display an extended IP ACL that is identified by the access list number.
  - **<int 100-199>** - Enter the extended IP ACL access list number used here. This value must be between 100 and 199.
- **named**- (Optional) Specifies to display an IP ACL that is identified by its name.
  - **<name 1-31>** - Enter the IP ACL name used here. This parameter is a case-sensitive alphanumeric field. This name can be up to 31 characters long.

ipv6 - Specifies to display an IPv6 ACL that is identified by its name.

- **<name 1-31>** - (Optional) Enter the IPv6 ACL name used here. This parameter is a case-sensitive alphanumeric field. This name can be up to 31 characters long.

Restrictions

None.

Example

To display a summary of MAC access list:

```
DWS-3160-24PC:admin#show wireless access_list mac
Command: show wireless access_list mac

 Current number of all ACLs: 9
 Maximum number of all ACLs: 100

 MAC ACL Name                     Rules
 -------------------------------  -----
 macacl                           0
 aclMac                           2

 Total MAC ACLs: 2

DWS-3160-24PC:admin#
```

To display all details of the rules that are defined for a MAC ACL:

```
DWS-3160-24PC:admin#show wireless access_list mac aclMac
Command: show wireless access_list mac aclMac

ACL Name: aclMac

Rule Number: 1
Action                                        : permit
Match Every                                   : TRUE

Rule Number: 2
Action                                        : permit
Match Every                                   : FALSE
Destination MAC Address                       : 00-ED-12-BA-34-CF
Destination MAC Mask                          : FF-FF-FF-FF-00-00
Ethertype                                     : ipv6

Total Rules : 2

DWS-3160-24PC:admin#
```

To display a summary of the IP access list:

```
DWS-3160-24PC:admin#show wireless access_list ip
Command: show wireless access_list ip

 Current number of all ACLs: 9
 Maximum number of all ACLs: 100

 IP ACL ID/Name                   Rules
 -------------------------------- -----
 1                                0
 5                                1
 100                              2
 ipacl                            0
 aclIPNamed-1                     2

Total IP ACLs: 5

DWS-3160-24PC:admin#
```

To display all the details of the rules that are defined for an IP extended ACL:

```
DWS-3160-24PC:admin#show wireless access_list ip extended 100
Command: show wireless access_list ip extended 100

Rule Number: 1
Action                                        : permit
Match Every                                   : TRUE

Rule Number: 2
Action                                        : permit
Match Every                                   : FALSE
Protocol                                      : 6(tcp)
Source L4 Port Keyword                        : 80(http)

Total Rules : 2

DWS-3160-24PC:admin#
```

To display a summary of the IPv6 access list:

```
DWS-3160-24PC:admin#show wireless access_list ipv6
Command: show wireless access_list ipv6

 Current number of all ACLs: 9
 Maximum number of all ACLs: 100

 IPv6 ACL Name                      Rules
 --------------------------------   -----
 ipv6acl                            0
 aclIpv6-1                          2

 Total IPv6 ACLs: 2

DWS-3160-24PC:admin#
```

To display all the details of the rules that are defined for an IPv6 ACL:

```
DWS-3160-24PC:admin#show wireless access_list ipv6 aclIpv6-1
Command: show wireless access_list ipv6 aclIpv6-1

ACL Name: aclIpv6-1

Rule Number: 1
Action                             : deny
Match Every                        : TRUE

Rule Number: 2
Action                             : deny
Match Every                        : FALSE
Source IP Address                  : 2001:FECD:BA23:CD1F:DCB1:1010:9234:4088/22

Total Rules : 2

DWS-3160-24PC:admin#
```

92-15 show wireless diffserv

Description

This command is used to display the wireless DiffServ general status information, a list of all the defined wireless DiffServ classes, all configuration information of the specified class, a list of all defined wireless DiffServ policies or all configuration information for the specified policy.

Format

show wireless diffserv {[class_map {class_name <name 1-31>} | policy_map {policy_name <name 1-31>}]}

Parameters

class_map - (Optional) Specifies to display the DiffServ class map(s) information.
class_name - Specifies the name of DiffServ class to be displayed.
<name 1-31> - Enter the name of DiffServ class, to be displayed, here. This name can be

up to 31 characters long. The name is a case sensitive alphanumeric string that uniquely identifies an existing wireless DiffServ class.

policy_map - (Optional) Specifies to display the DiffServ policy map(s) information.
policy_name - Specifies the name of DiffServ policy to be displayed.
<name 1-31> - Enter the name of DiffServ policy, to be displayed, here. This name can be up to 31 characters long. The name is a case sensitive alphanumeric string that uniquely identifies an existing wireless DiffServ class.

Restrictions

None.

Example

To display the wireless DiffServ general status information:

```
DWS-3160-24PC:admin#show wireless diffserv
Command: show wireless diffserv

Class Table Size Current/Max                  : 5 / 32
Class Rule Table Size Current/Max             : 2 / 192
Policy Table Size Current/Max                 : 4 / 64
Policy Instance Table Size Current/Max        : 1 / 640
Policy Attribute Table Size Current/Max       : 0 / 1280

DWS-3160-24PC:admin#
```

To display a list of all defined wireless DiffServ classes:

```
DWS-3160-24PC:admin#show wireless diffserv class_map
Command: show wireless diffserv class_map

                                 Class L3
           Class Name            Type  Proto      Reference Class Name
 ------------------------------- ----- ----- -------------------------------
 cm1                             All   IPv4
 cm2                             All   IPv4
 cm3                             All   IPv6
 cm30                            All   IPv4
 cm31                            All   IPv4

Total Classes : 5

DWS-3160-24PC:admin#
```

To display configuration information of the specified class:

```
DWS-3160-24PC:admin#show wireless diffserv class_map class_name cm31
Command: show wireless diffserv class_map class_name cm31

Class Name                                    : cm31
Class Type                                    : All
Class Layer3 Protocol                         : IPv4

      Match Criteria                           Values
---------------------------- -------------------------------------------
 IP TOS                       0x11 (0x22)

DWS-3160-24PC:admin#
```

To display a list of all defined wireless DiffServ policy maps:

```
DWS-3160-24PC:admin#show wireless diffserv policy_map
Command: show wireless diffserv policy_map

           Policy Name           Policy Type           Class Members
 ------------------------------- ------------ --------------------------------
 pm1                             In           cm1
 pm2                             In           cm2

Total Policies : 2

DWS-3160-24PC:admin#
```

To display configuration information for the specified policy:

```
DWS-3160-24PC:admin#show wireless diffserv policy_map policy_name df_policy1
Command: show wireless diffserv policy_map policy_name df_policy1

Policy Name                                   : df_policy1
Policy Type                                   : In

Class Name                                    : cm30
Best Effort will be used.

DWS-3160-24PC:admin#
```

Chapter 93 Wireless RF Scan AP Status Command List

delete wireless ap_rf_scan_list

93-1 delete wireless ap_rf_scan_list

Description

This command is used to delete all entries from the RF scan list. The RF scan list is data maintained for all access points known by the Wireless Switch via the RF scan data, obtained from the managed access points.

Format

delete wireless ap_rf_scan_list

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To delete all entries from the RF scan list:

```
DWS-3160-24PC:admin#delete wireless ap_rf_scan_list
Command: delete wireless ap_rf_scan_list

Are you sure you want to delete all RF Scan entries? (y/n) y
delete wireless ap_rf_scan_list

All RF Scan entries deleted.

Success.

DWS-3160-24PC:admin#
```

Chapter 94 Wireless Switch Channel and Power Command List

config wireless channel_plan [an | bgn] [mode [interval | manual | time] | interval [<int 6-24> | default] | time [<start_time hh:mm> | default] | history depth [<int 0-10> | default] | action [apply | clear | start]]
config wireless power_plan [mode [interval | manual] | interval [<int 15-1440> | default] | action [apply | clear | start]]
show wireless channel_plan [an | bgn]
show wireless channel_plan history [an | bgn]
show wireless channel_plan proposed [an | bgn]
show wireless power_plan
show wireless power_plan proposed

94-1 config wireless channel_plan

Description

This command is used to configure automatic wireless channel planning on this Switch.

Format

config wireless channel_plan [an | bgn] [mode [interval | manual | time] | interval [<int 6-24> | default] | time [<start_time hh:mm> | default] | history depth [<int 0-10> | default] | action [apply | clear | start]]

Parameters

an - Specifies to configure the wireless channel plan mode for 802.11a/n. **bgn** - Specifies to configure the wireless channel plan mode for 802.11b/g/n.
mode - Specifies the wireless channel plan mode for each 802.11a/n and 802.11b/g/n frequency band. **interval** - Specifies to compute and apply new wireless channel plans at the configured interval. **manual** - Specifies to compute and apply new wireless channel plans only when requested via the user interface. This is the default option. **time** - Specifies to compute and apply new wireless channel plans at the configured time.
interval - Specifies the wireless channel plan interval. **<int 6-24>** - Enter the wireless channel plan interval used here. This value must be between 6 and 24 hours. The default value is 6 hours. **default** - Specifies that the default value will be used.
time - Specifies the wireless channel plan time. **<start_time hh:mm>** - Enter the wireless channel plan starting time here. This value must follow the hh:mm format. The default value is 00:00. **default** - Specifies that the default value will be used.
history depth - Specifies the number of wireless channel plan history iterations. **<int 0-10>** - Enter the number of wireless channel plan history iterations used here. This value must be between 0 and 10. The default value is 5. **default** - Specifies that the default value will be used.
action - Specifies to request manual wireless channel plan actions for each 802.11a/n and 802.11b/g/n frequency band. **apply** - Specifies to apply the entire proposed wireless channel plan. **clear** - Specifies to clear the current proposed wireless channel plan.

start - Specifies to compute a new proposed wireless channel plan.

Restrictions

Only Administrators can issue this command.

Example

To configure the wireless channel plan mode:

```
DWS-3160-24PC:admin#config wireless channel_plan an mode interval
Command: config wireless channel_plan an mode interval

Success.

DWS-3160-24PC:admin#
```

To configure the wireless channel plan interval:

```
DWS-3160-24PC:admin#config wireless channel_plan an interval 24
Command: config wireless channel_plan an interval 24

Success.

DWS-3160-24PC:admin#
```

To configure the history depth:

```
DWS-3160-24PC:admin#config wireless channel_plan an history depth 10
Command: config wireless channel_plan an history depth 10

Success.

DWS-3160-24PC:admin#
```

To apply the entire proposed wireless channel plan:

```
DWS-3160-24PC:admin# config wireless channel_plan an action apply
Command: config wireless channel_plan an action apply

Success.

DWS-3160-24PC:admin#
```

94-2 config wireless power_plan

Description

This command is used to configure the power plan mode, the adjustment interval, and manages manual power adjustments for the managed APs.

Format

config wireless power_plan [mode [interval | manual] | interval [<int 15-1440> | default] | action [apply | clear | start]]

Parameters

mode - Specifies the power plan mode for managed APs.
- **interval** - Specifies to compute and apply power adjustments at the configured interval.
- **manual** - Specifies to compute and apply power adjustments only when requested via the user interface. This is the default option.

interval - Specifies the power adjustment interval.
- **<int 15-1440>** - Enter the power adjustment interval here. This value must be between 15 and 1440 minutes. The default value is 15 minutes.
- **default** - Specifies that the default value will be used.

action - Specifies to trigger manual power adjustment actions on the managed APs.
- **apply** - Specifies to apply the proposed power adjustments.
- **clear** - Specifies to clear the proposed power adjustments.
- **start** - Specifies to compute new proposed power adjustments.

Restrictions

Only Administrators can issue this command.

Example

To configure the power plan mode:

```
DWS-3160-24PC:admin#config wireless power_plan mode interval
Command: config wireless power_plan mode interval

Success.

DWS-3160-24PC:admin#
```

To configure the power plan interval:

```
DWS-3160-24PC:admin#config wireless power_plan interval 24
Command: config wireless power_plan interval 24

Success.

DWS-3160-24PC:admin#
```

To apply the power adjustment on managed APs:

```
DWS-3160-24PC:admin# config wireless power_plan action apply
Command: config wireless power_plan action apply

Success.

DWS-3160-24PC:admin#
```

94-3 show wireless channel_plan

Description

This command is used to display the configuration for automatic channel planning.

Format

show wireless channel_plan [an | bgn]

Parameters

an - Specifies that the configured wireless channel plan mode for 802.11a/n will be displayed.

bgn - Specifies that the configured wireless channel plan mode for 802.11b/g/n will be displayed.

Restrictions

None.

Example

To display the configured wireless channel plan mode for 802.11a/n

```
DWS-3160-24PC:admin#show wireless channel_plan an
Command: show wireless channel_plan an

---------------------------------------------------------------------
*             Channel Plan                                          *
---------------------------------------------------------------------
802.11a Channel Configuration:

Channel Plan Mode                             : Manual
Channel Plan Interval (hours)                 : 24
Channel Plan Fixed Time (hh:mm)               : 00:00
Channel Plan History Depth                    : 10

DWS-3160-24PC:admin#
```

94-4 show wireless channel_plan history

Description

This command is used to display a history for the automatic channel algorithm.

Format

show wireless channel_plan history [an | bgn]

Parameters

history - Specifies to display the history of the automatic channel algorithm. The channel plan type argument must be specified. A channel history is maintained separately for each radio frequency.

an - Specifies that the configured wireless channel plan mode for 802.11a/n will be displayed.

bgn - Specifies that the configured wireless channel plan mode for 802.11b/g/n will be displayed.

Restrictions

None.

Example

To display the channel plan history:

```
DWS-3160-24PC:admin# show wireless channel_plan history an
Command: show wireless channel_plan history an

Operational Status                            : Active
Last Iteration                                : 0
Last Algorithm Time                           : -----

AP MAC Address    Location                         Radio Iteration channel
----------------- -------------------------------  ----- ------- -------
00-22-B0-3D-A9-40                                  2      1       1

DWS-3160-24PC:admin#
```

94-5 show wireless channel_plan proposed

Description

This command is used to display a proposed channel plan change for a manual request to run the channel algorithm.

Format

show wireless channel_plan proposed [an | bgn]

Parameters

proposed - Specifies to display proposed channel plan changes for a manual request to run the channel algorithm. The channel plan type argument must be specified.

an - Specifies that the configured wireless channel plan mode for 802.11a/n will be displayed.

bgn - Specifies that the configured wireless channel plan mode for 802.11b/g/n will be displayed.

Restrictions

None.

Example

To display the proposed channel plan:

```
DWS-3160-24PC:admin# show wireless channel_plan proposed an
Command: show wireless channel_plan proposed an

Current Status                              : Algorithm Completed


                                               Current  New
AP MAC Address    Location                         Radio channel channel
----------------- --------------------------------  ----- ------- -------
00-22-B0-3D-A9-40                                  2        6      11
00-22-B0-3D-AA-C0                                  1       36      44

DWS-3160-24PC:admin#
```

94-6 show wireless power_plan

Description

This command is used to display the status and configuration for automatic power adjustments.

Format

show wireless power_plan

Parameters

None.

Restrictions

None.

Example

To display the power plan global status:

```
DWS-3160-24PC:admin#show wireless power_plan
Command: show wireless power_plan

Power Adjustment Mode                          : Interval
Power Adjustment Interval (minutes)            : 24

DWS-3160-24PC:admin#
```

a. show wireless power_plan proposed

Description

This command is used to specify the proposed power adjustments for a manual request to run the power algorithm. The proposed power changes may be cleared or applied using the wireless power-plan command.

Format

show wireless power_plan proposed

Parameters

None.

Restrictions

None.

Example

To display the proposed power plan:

```
DWS-3160-24PC:admin# show wireless power_plan proposed
Command: show wireless power_plan proposed

Current Status                                : Algorithm Completed


                                                         Current New
AP MAC Address    Location                         Radio Power   Power
----------------- --------------------------------  ----- ------- -------
00-22-B0-3D-A9-40                                  2     80      90
00-22-B0-3D-AA-C0                                  1     60      70
00-22-B0-3D-AA-C0                                  2     80      90
00-22-B0-3D-AB-40                                  2     80      90

DWS-3160-24PC:admin#
```

Chapter 95 Wireless Switch Command List

enable wireless

disable wireless

create wireless discovery [ip <ipaddr> | vlan <vlanid 1-4094>]

delete wireless discovery [ip [<ipaddr> | all] | vlan [<vlanid 1-4094> | all]]

config wireless discovery {l3 [enable | disable] | l2 [enable | disable]}(1)

create wireless known_client <macaddr>

delete wireless known_client <macaddr>

config wireless known_client <macaddr> [name <name 32> | action [global_action | grant | deny]]

create wireless oui_database <ouival> {<desc 1-32>}

delete wireless oui_database <ouival>

config wireless oui_database <ouival> <desc 1-32>

config wireless acknowledge_rogue [<macaddr> | all]

config wireless agetime [ad_hoc [<int 0-168> | default] | ap_failure [<int 0-168> | default] | rf_scan [<int 0-168> | default] | detected_client [<int 0-168> | default] | ap_provisioning_db [<int 0-240> | default]]

config wireless ap_authentication [enable | disable]

config wireless ap_auto_upgrade [enable | disable]

config wireless ap_client_qos [enable | disable]

config wireless ap_validation [local | radius]

config wireless auto_ip_assign [enable | disable]

config wireless client roam_timeout [<int 1-120> | default]

config wireless cluster priority <int 0-255>

config wireless country_code [<country_code> | default]

config wireless dist_tunnel {max_clients [<int 1-8000> | default] | idle_timeout [<int 30-3600> | default] | max_timeout [<int 30-86400> | default] | mcast_repl [<int 1-1024> | default]}(1)

config wireless ip_control_port [<int 1-65000> | default]

config wireless mac_authentication_mode [white_list | black_list]

config wireless peer_group [<int 1-255> | default]

config wireless radius [accounting [enable | disable]]

config wireless static_ip [<ipaddr> | clear]

config wireless trap [enable | disable] [all | ap_failure | ap_state | client_failure | client_state | peer_ws | rf_scan | rogue_ap | wids_status | ws_status]

config wireless tunnel_mtu [1500 | 1520 | default]

clear wireless statistics

show wireless

show wireless agetime

show wireless ap_capability {[[any | hw_dwl8600 | hw_dwl3600 | hw_dwl6600] radio <int 1-2> | image_table | dual_boot]}

show wireless ap_image availability

show wireless country_code

show wireless discovery {[ip_list | vlan_list]}

show wireless dist_tunnel {statistics}

show wireless known_client

show wireless mac_authentication_mode

show wireless multicast tx_rates [a | bg]

show wireless oui_database {<ouival>}

show wireless radius

show wireless rates [a | bg]

show wireless statistics

show wireless status
show wireless switch [<ipaddr> | local] {[statistics | client]}
show wireless trap
show wireless tunnel_mtu

95-1 enable wireless

Description

This command is used to enable the Wireless Switch functionality.

Format

enable wireless

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the Wireless Switch functionality:

```
DWS-3160-24PC:admin#enable wireless
Command: enable wireless

Success.

DWS-3160-24PC:admin#
```

95-2 disable wireless

Description

This command is used to disable the Wireless Switch functionality.

Format

disable wireless

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the Wireless Switch functionality:

```
DWS-3160-24PC:admin#disable wireless
Command: disable wireless

Success.

DWS-3160-24PC:admin#
```

95-3 create wireless discovery

Description

This command is used to add an IP address to the list of addresses used globally by the Wireless Switch. The Switch polls each address in the list to discover new access points and peers. This command also adds VLAN IDs that will be used to send Layer 2 discovery multicast frames. Up to 16 VLAN IDs can be configured. By default, there is one entry in the list. The IP list is used when the discovery via IP polling feature is enabled. The VLAN list is used when the discovery via Layer 2 multicast feauters is enabled.

Format

create wireless discovery [ip <ipaddr> | vlan <vlanid 1-4094>]

Parameters

ip - Specifies that a valid IP address will be used.
  <ipaddr> - Enter the valid IP address used here.

vlan - Specifies that the VLAN ID will be used.
  <vlanid 1-4094> - Enter the VLAN ID used here. This value must be between 1 and 4094.

Restrictions

Only Administrators can issue this command.

Example

To configure an IP address to discovered:

```
DWS-3160-24PC:admin#create wireless discovery ip 10.1.2.3
Command: create wireless discovery ip 10.1.2.3

Success.

DWS-3160-24PC:admin#
```

To configure a VLAN ID for Layer 2 discovery:

```
DWS-3160-24PC:admin#create wireless discovery vlan 3
Command: create wireless discovery vlan 3

Success.

DWS-3160-24PC:admin#
```

95-4 delete wireless discovery

Description

This command is used to delete entries from the Layer 3 IP polling list or the VLAN discovery list.

Format

delete wireless discovery [ip [<ipaddr> | all] | vlan [<vlanid 1-4094> | all]]

Parameters

ip - Specifies that a specific IP address will be deleted from the polling list.
- **<ipaddr>** - Enter the IP address that will be deleted, here.
- **all** - Specifies that all IP addresses will be deleted from the polling list.

vlan - Specifies that a specific VLAN ID will be deleted from the discovery list.
- **<vlanid 1-4094>** - Enter the VLAN ID, that will be deleted, here. This value must be between 1 and 4094.
- **all** - Specifies that all VLAN IDs will be deleted from the discovery list.

Restrictions

Only Administrators can issue this command.

Example

To delete a specific IP address from the polling list:

```
DWS-3160-24PC:admin#delete wireless discovery ip 10.1.1.1
Command: delete wireless discovery ip 10.1.1.1

Success.

DWS-3160-24PC:admin#
```

To delete a specific VLAN ID from the discovery list:

```
DWS-3160-24PC:admin#delete wireless discovery vlan 2
Command: delete wireless discovery vlan 2

Success.

DWS-3160-24PC:admin#
```

95-5 config wireless discovery

Description

This command is used to enable various methods used for the discovery of APs and peer Switches.

Format

config wireless discovery {l3 [enable | disable] | l2 [enable | disable]}(1)

Parameters

l3 - (Optional) Specifies the state of Layer 3, IP-based, discovery of APs and peer Switches.
- **enable** - Specifies that Layer 3, IP-based, discovery of APs and peer Switches, will be enabled.
- **disable** - Specifies that Layer 3, IP-based, discovery of APs and peer Switches, will be disabled.

l2 - (Optional) Specifies the state of Layer 2, MAC-based, discovery of APs and peer Switches.
- **enable** - Specifies that Layer 2, MAC-based, discovery of APs and peer Switches, will be enabled.
- **disable** - Specifies that Layer 2, MAC-based, discovery of APs and peer Switches, will be disabled.

Although the above mentioned parameters are all listed as optional, the user is required to at least select one parameter to successfully utilize this command.

Restrictions

Only Administrators can issue this command.

Example

To enable Layer 3, IP-based, discovery of APs and peer Switches:

```
DWS-3160-24PC:admin#config wireless discovery l3 enable
Command: config wireless discovery l3 enable

Success.

DWS-3160-24PC:admin#
```

To enable Layer 2, MAC-based, discovery of APs and peer Switches.

```
DWS-3160-24PC:admin#config wireless discovery l2 enable
Command: config wireless discovery l2 enable

Success.

DWS-3160-24PC:admin#
```

95-6 create wireless known_client

Description

This command is used to add a client MAC address to the local known client database.

Format

create wireless known_client <macaddr>

Parameters

<macaddr> - Enter a valid MAC address of a physical wireless client here.

Restrictions

Only Administrators can issue this command.

Example

To add the MAC address of ‘00-18-DE-D7-B4-C1’ to the local known client database:

```
DWS-3160-24PC:admin#create wireless known_client 00-18-DE-D7-B4-C1
Command: create wireless known_client 00-18-DE-D7-B4-C1

Success.

DWS-3160-24PC:admin#
```

95-7 delete wireless known_client

Description

This command is used to delete a client MAC address from the local known client database.

Format

delete wireless known_client <macaddr>

Parameters

<macaddr> - Enter a valid MAC address of a physical wireless client here.

Restrictions

Only Administrators can issue this command.

Example

To delete the MAC address of ‘00-18-DE-D7-B4-C1’ from the local known client database:

```
DWS-3160-24PC:admin#delete wireless known_client 00-18-DE-D7-B4-C1
Command: delete wireless known_client 00-18-DE-D7-B4-C1

Success.

DWS-3160-24PC:admin#
```

95-8 config wireless known_client

Description

This command is used to configure a client MAC address in the local known client database. This action indicates whether to grant, deny or use global action for MAC authentication of the client.

If the global MAC Authentication action is configured as “White List”, then any wireless client with a MAC address, specified in the list, and are not explicitly denied access, is granted access. If a MAC address is not in the list, then the access to this client is denied.

If the global MAC Authentication action is configured as “Black List”, then any wireless client with a MAC address, specified in the list, and are not explicitly granted access, is denied access. If a MAC address is not in the list, then the access to this client is granted.

Format

config wireless known_client <macaddr> [name <name 32> | action [global_action | grant | deny]]

Parameters

<macaddr> - Enter a valid MAC address of a physical wireless client here.

name - Specifies the name of the physical wireless client, used for identification, here.
- **<name 32>** - Enter the name of the physical wireless client, used for identification, here. This name can be up to 32 alphanumeric characters long.

action - Specifies the type of MAC authentication action to be taken for the specified physical wireless client.
- **global_action** - Specifies that the MAC authentication action, for the specified physical wireless client, will be set as global action. This is also the default value.
- **grant** - Specifies that the MAC authentication action, for the specified physical wireless client, will be set as grant.
- **deny** - Specifies that the MAC authentication action, for the specified physical wireless client, will be set as deny.

Restrictions

Only Administrators can issue this command.

Example

To configure a known client name:

```
DWS-3160-24PC:admin#config wireless known_client 00-18-DE-D7-B4-C1 name
reception
Command: config wireless known_client 00-18-DE-D7-B4-C1 name reception

Success.

DWS-3160-24PC:admin#
```

To configure a deny action for a known client:

```
DWS-3160-24PC:admin#config wireless known_client 00-18-DE-D7-B4-C1 action deny
Command: config wireless known_client 00-18-DE-D7-B4-C1 action deny

Success.

DWS-3160-24PC:admin#
```

95-9 create wireless oui_database

Description

This command is used to add a new entry to the OUI database. Each entry consists of an OUI value, which is composed out of the higher three octets of the Ethernet MAC address of the AP or Client and the organization name for the OUI, which is a 32-byte string.

Format

create wireless oui_database <ouival> {<desc 1-32>}

Parameters

<ouival> - Enter the OUI Value, which is composed of the higher three octets of the Ethernet MAC address of the vendor AP or Client, here.

<desc 1-32> - (Optional) Enter the organization name for the OUI here. This name can be up to 32 alphanumeric characters long.

Restrictions

Only Administrators can issue this command.

Example

To create an OUI value:

```
DWS-3160-24PC:admin#create wireless oui_database 00:00:01 VendorName
Command: create wireless oui_database 00:00:01 VendorName

Success.

DWS-3160-24PC:admin#
```

95-10 delete wireless oui_database

Description

This command is used to delete the OUI entry, of the specified OUI value, from the local OUI database.

Format

delete wireless oui_database <ouival>

Parameters

<ouival> - Enter the OUI Value, which is composed of the higher three octets of the Ethernet MAC address of the vendor AP or Client, here.

Restrictions

Only Administrators can issue this command.

Example

To delete an OUI value:

```
DWS-3160-24PC:admin#delete wireless oui_database 00:00:01
Command: delete wireless oui_database 00:00:01

Success.

DWS-3160-24PC:admin#
```

95-11 config wireless oui_database

Description

This command is used to configure the name of an OUI value.

Format

config wireless oui_database <ouival> <desc 1-32>

Parameters

<ouival> - Enter the OUI Value, which is composed of the higher three octets of the Ethernet MAC address of the vendor AP or Client, here.

<desc 1-32> - Enter the organization name, for the OUI, here. This name can be up to 32 alphanumeric characters long.

Restrictions

Only Administrators can issue this command.

Example

To configure the OUI database:

```
DWS-3160-24PC:admin#config wireless oui_database 00:00:01 D-Link
Command: config wireless oui_database 00:00:01 D-Link

Success.

DWS-3160-24PC:admin#
```

95-12 config wireless acknowledge_rogue

Description

This command is used to acknowledge a rogue AP's in the RF Scan database. This command can also be used to acknowledge all rogue APs.

Format

config wireless acknowledge_rogue [<macaddr> | all]

Parameters

<macaddr> - Enter a valid MAC address of a rogue AP here.
all - Specifies that all rogue APs will be acknowledged.

Restrictions

Only Administrators can issue this command.

Example

To acknowledge all rogue APs:

```
DWS-3160-24PC:admin#config wireless acknowledge_rogue all
Command: config wireless acknowledge_rogue all

 All rogue APs acknowledged.

Success.

DWS-3160-24PC:admin#
```

95-13 config wireless agetime

Description

This command is used to configure database entry age times for the Wireless Switch. A time value of 0 indicates that entries in the corresponding database will not age and that the user must manually delete them.

Format

config wireless agetime [ad_hoc [<int 0-168> | default] | ap_failure [<int 0-168> | default] | rf_scan [<int 0-168> | default] | detected_client [<int 0-168> | default] | ap_provisioning_db [<int 0-240> | default]]

Parameters

ad_hoc - Specifies the time to maintain an entry in the ad hoc client network list. A value of 0 indicates that the entries should never age out.
  <int 0-168> - Enter the time to maintain and entry in the ad hoc client network list here. This value must be between 0 and 168 hours. This default value is 24 hours.
  default - Specifies that the default value will be used.

ap_failure - Specifies the time to maintain an entry in the AP association and authentication failure list. A value of 0 indicates that the entries should never age out.

<int 0-168> - Enter the time to maintain an entry in the AP association and authentication failure list here. This value must be between 0 and 168 hours. The default value is 24 hours.

default - Specifies that the default value will be used.

rf_scan - Specifies the time to maintain an entry obtained from an RF scan. A value of 0 indicates that the entries should never age out.

<int 0-168> - Enter the time to maintain an entry obtained from an RF scan here. This value must be between 0 and 168 hours. The default value is 24 hours.

default - Specifies that the default value will be used.

detected_client - Specifies the time to maintain an entry in the detected client(s) database. A value of 0 indicates that the entries should never age out.

<int 0-168> - Enter the time to maintain an entry in the detected client(s) database here. This value must be between 0 and 168 hours. The default value is 24 hours.

default - Specifies that the default value will be used.

ap_provisioning_db - Specifies the time to maintain an entry in the AP provisioning database. A value of 0 indicates that the entries should never age out.

<int 0-240> - Enter the time to maintain an entry in the AP provisioning database here. This value must be between 0 and 240 hours. The default value is 72 hours.

default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To configure the entry age for the ad hoc network status:

```
DWS-3160-24PC:admin#config wireless agetime ad_hoc 20
Command: config wireless agetime ad_hoc 20

Success.

DWS-3160-24PC:admin#
```

To disable the age out value for AP failure status entries:

```
DWS-3160-24PC:admin#config wireless agetime ap_failure 0
Command: config wireless agetime ap_failure 0

Success.

DWS-3160-24PC:admin#
```

To configure the default entry age for the AP provisioning status:

```
DWS-3160-24PC:admin#config wireless agetime ap_provisioning_db default
Command: config wireless agetime ap_provisioning_db default

Success.

DWS-3160-24PC:admin#
```

95-14 config wireless ap_authentication

Description

This command is used to enable or disables AP authentication. When enabled, all APs are required to authenticate to the Wireless Switch using a password upon discovery. When disabled, APs are not required to authenticate to the Wireless Switch upon discovery.

Format

config wireless ap_authentication [enable | disable]

Parameters

enable - Specifies that AP authentication mode will be enabled.
disable - Specifies that AP authentication mode will be disabled.

Restrictions

Only Administrators can issue this command.

Example

To enable the AP authentication mode:

```
DWS-3160-24PC:admin#config wireless ap_authentication enable
Command: config wireless ap_authentication enable

Success.

DWS-3160-24PC:admin#
```

95-15 config wireless ap_auto_upgrade

Description

This command is used to globally enable or disable the AP automatic upgrade mode on the Switch. This feature will be enforced on all supported APs.

When the AP’s automatic upgrade mode is enabled, the Switch, that manages the AP, will automatically load the code image for the AP stored on the Switch. If the code image of the supported AP hardware type is not available, this step will be skipped and the AP will toggle to a managed mode. The administrator should then load the code manually on this AP.

When the AP’s automatic upgrade mode is disabled, the AP code upgrade is never initiated automatically by the Switch.

Format

config wireless ap_auto_upgrade [enable | disable]

Parameters

enable - Specifies that the AP automatic upgrade option will be enabled.
disable - Specifies that the AP automatic upgrade option will be disabled. This is the default

option.

Restrictions

Only Administrators can issue this command.

Example

To enable the AP automatic upgrade mode:

```
DWS-3160-24PC:admin#config wireless ap_auto_upgrade enable
Command: config wireless ap_auto_upgrade enable

Success.

DWS-3160-24PC:admin#
```

95-16 config wireless ap_client_qos

Description

This command is used to enable or disable AP client QoS operation globally for the wireless Switch. When enabled, and when the network client QoS mode is also enabled, clients associated to that network may have one or more of the following QoS characteristics in effect in the down and/or up directions for access control, bandwidth limiting, and differentiated services.

This command takes effect on an AP without requiring that the AP profile be re-applied.

Format

config wireless ap_client_qos [enable | disable]

Parameters

enable - Specifies that the AP Client QoS mode will be enabled.
disable - Specifies that the AP Client QoS mode will be disabled. This is the default option.

Restrictions

Only Administrators can issue this command.

Example

To enable the AP Client QoS mode:

```
DWS-3160-24PC:admin#config wireless ap_client_qos enable
Command: config wireless ap_client_qos enable

Success.

DWS-3160-24PC:admin#
```

95-17 config wireless ap_validation

Description

This command is used to configure whether to use the local valid AP database or a RADIUS server to validate newly discovered APs.

Format

config wireless ap_validation [local | radius]

Parameters

local - Specifies that the local database will be used for validating discovered APs.
radius - Specifies that the RADIUS server will be used for validating discovered APs.

Restrictions

Only Administrators can issue this command.

Example

To configure AP validation mode as RADIUS:

```
DWS-3160-24PC:admin#config wireless ap_validation radius
Command: config wireless ap_validation radius

Success.

DWS-3160-24PC:admin#
```

95-18 config wireless auto_ip_assign

Description

This command is used to enable or disable the automatic IP address assignment mode for the wireless Switch. Use this command to allow the wireless feature to automatically assign itself an IP address from one of the active interfaces. If this option is cleared, you must manually assign the IP address in the Switch Static IP Address field.

Format

config wireless auto_ip_assign [enable | disable]

Parameters

enable - Specifies that the automatic IP address assignment mode for the wireless Switch will be enabled.
disable - Specifies that the automatic IP address assignment mode for the wireless Switch will be disabled. This is the default option.

Restrictions

Only Administrators can issue this command.

Example

To enable the automatic IP assignment feature:

```
DWS-3160-24PC:admin#config wireless auto_ip_assign enable
Command: config wireless auto_ip_assign enable

Success.

DWS-3160-24PC:admin#
```

95-19 config wireless client roam_timeout

Description

This command is used to configure the maximum duration for client entry detainment in the client association database after disassociating it from a managed AP. The roam timeout is the time in seconds after disassociation after which an entry will be deleted from the managed AP client association database.

Format

config wireless client roam_timeout [<int 1-120> | default]

Parameters

<int 1-120> - Enter the roam timeout value used here. This value must be between 1 and 120 seconds. The default value is 30 seconds.

default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To configure the client's roaming timeout value:

```
DWS-3160-24PC:admin#config wireless client roam_timeout 60
Command: config wireless client roam_timeout 60

Success.

DWS-3160-24PC:admin#
```

95-20 config wireless cluster priority

Description

This command is used to configure the cluster priority of the Switch. This configuration is used to change the preference level of the Switch to select or unselect it as the Cluster Controller. A higher number indicates a higher preference.

Format

config wireless cluster priority <int 0-255>

Parameters

<int 0-255> - Enter the preference level for the Cluster Controller election here. This value must be between 0 and 255. The default value is 1.

Restrictions

Only Administrators can issue this command.

Example

To configure the cluster priority:

```
DWS-3160-24PC:admin#config wireless cluster priority 1
Command: config wireless cluster priority 1

Success.

DWS-3160-24PC:admin#
```

95-21 config wireless country_code

Description

This command is used to globally configure the country code for the Wireless Switch and all managed access points. The code may be entered in either upper or lower case. When you change the country code, the wireless function is disabled and re-enabled automatically.

Format

config wireless country_code [<country_code> | default]

Parameters

<country_code> - Enter the valid country code value here. The default value is 'US'.
default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To configure the country code:

```
DWS-3160-24PC:admin#config wireless country_code default
Command: config wireless country_code default

The default country code (US) will be used as a result of this command.

The WLAN application is currently enabled.
Changing the country code will disable it on the switch, then re-enable it.
Any channel and radio mode settings invalid for the regulatory domain
will be reset to default values.

Are you sure you want to change the country code? (y/n) y

Country code saved.

Success.

DWS-3160-24PC:admin#
```

95-22 config wireless dist_tunnel

Description

This command is used to configure the Layer 2 Distributed Tunneling parameters.

Format

config wireless dist_tunnel {max_clients [<int 1-8000> | default] | idle_timeout [<int 30-3600> | default] | max_timeout [<int 30-86400> | default] | mcast_repl [<int 1-1024> | default]}(1)

Parameters

max_clients - (Optional) Specifies the maximum number of distributed tunneling clients that can roam away from the Home AP at the same time.
- **<int 1-8000>** - Enter the maximum number of clients used here. This value must be between 1 and 8000. The default value is 128.
- **default** - Specifies that the default value will be used.

idle_timeout - (Optional) Specifies the number of seconds of no activity by the client before the tunnel to that client is terminated and the client is forced to change its IP address.
- **<int 30-3600>** - Enter the idle timeout value, used for the tunnel, here. This value must be between 30 and 3600. The default value is 120.
- **default** - Specifies that the default value will be used.

max_timeout - (Optional) Specifies the number of seconds before the tunnel to the roamed client is terminated and the client is forced to change its IP address.
- **<int 30-86400>** - Enter the maximum timeout value used here. This value must be between 30 and 86400. The default value is 7200.
- **default** - Specifies that the default value will be used.

mcast_repl - (Optional) Specifies the maximum number of tunnels to which a multicast frame is copied on the Home AP.
- **<int 1-1024>** - Enter the number of multicast replications here. This value must be between 1 and 1024. The default value is 128.
- **default** - Specifies that the default value will be used.

Although the above mentioned parameters are all listed as optional, the user is required to at least select one parameter to successfully utilize this command.

Restrictions

Only Administrators can issue this command.

Example

To configure the Layer 2 Distributed Tunneling parameters:

```
DWS-3160-24PC:admin#config wireless dist_tunnel max_clients 800 idle_timeout
100 max_timeout 300 mcast_repl 400
Command: config wireless dist_tunnel max_clients 800 idle_timeout 100
max_timeout 300 mcast_repl 400

Success.

DWS-3160-24PC:admin#
```

95-23 config wireless ip_control_port

Description

This command is used to configure the IP control data communication port. It configures the first IP port number within the range that the wireless system uses to send and receive IP traffic. By default the wireless system uses the IP port number 57775. When we change the base IP port number, the wireless feature will automatically be disabled and re-enabled. The default wireless IP port number is not sent as part of the global Switch configuration in the cluster configuration distribution command. Every Switch in the cluster must be configured independently with the new IP port number. When the wireless IP port number is changed from its default value on the Switch, then it must also be changed on the Access Points. The port number can be configured on the AP via an AP administrative command, or DHCP option 43, sub-option 3. If the port is configured via DHCP, then the DHCP setting supersedes the configured setting.

Format

config wireless ip_control_port [<int 1-65000> | default]

Parameters

<int 1-65000> - Enter the identifier value for the IP control port here. This value must be between 1 and 65000. The default value is 57775.

default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To configure the IP control data communication port:

```
DWS-3160-24PC:admin#config wireless ip_control_port 57775
Command: config wireless ip_control_port 57775

Success.

DWS-3160-24PC:admin#
```

95-24 config wireless mac_authentication_mode

Description

This command is used to configure the client MAC authentication mode for the Switch. The mode indicates whether MAC addresses, in the Known Client database, are granted or denied access. The MAC authentication mode is applied to the Known Client database configured either locally or on the RADIUS server.

Format

config wireless mac_authentication_mode [white_list | black_list]

Parameters

white_list - Specifies that access is granted only to clients with MAC addresses in the Known Client database. This is the default option.

black_list - Specifies that access is denied to clients with MAC addresses in the Known Client database.

Restrictions

Only Administrators can issue this command.

Example

To configure that MAC authentication mode as ‘black_list’:

```
DWS-3160-24PC:admin#config wireless mac_authentication_mode black_list
Command: config wireless mac_authentication_mode black_list

Success.

DWS-3160-24PC:admin#
```

95-25 config wireless peer_group

Description

This command is used to indicate the peer group for this Switch. There may be more than one group of peer Switches on the same WLAN. A peer group is created by configuring all peers within the group with the same identifier.

Format

config wireless peer_group [<int 1-255> | default]

Parameters

<int 1-255> - Enter the identifier for the peer Switch group here. This value must be between 1 and 255. The default value is 1.

default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To configure the peer Switch group ID:

```
DWS-3160-24PC:admin#config wireless peer_group 168
Command: config wireless peer_group 168

Success.

DWS-3160-24PC:admin#
```

95-26 config wireless radius

Description

This command is used to configure the global RADIUS setting.

NOTE: This command only configures the accounting status for wireless use.

Format

config wireless radius [accounting [enable | disable]]

Parameters

accounting - Specifies the state of the wireless RADIUS accounting feature.

enable - Specifies that the wireless RADIUS accounting feature will be enabled.

disable - Specifies that the wireless RADIUS accounting feature will be disabled. This is the default option.

Restrictions

Only Administrators can issue this command.

Example

To enable accounting for wireless clients:

```
DWS-3160-24PC:admin#config wireless radius accounting enable
Command: config wireless radius accounting enable

Success.

DWS-3160-24PC:admin#
```

95-27 config wireless static_ip

Description

This command is used to configure static IP addresses for the wireless Switch. An IP address must be the same as an IP address of an active routing interface in order for the wireless function to work. This IP address is used by the wireless Switch when the auto-ip-assign mode is disabled.

Format

config wireless static_ip [<ipaddr> | clear]

Parameters

<ipaddr> - Enter a valid IP address, for the wireless Switch, here.
clear - Specifies that the static IP address will reset to '0.0.0.0'.

Restrictions

Only Administrators can issue this command.

Example

To configure a static IP address for the wireless Switch:

```
DWS-3160-24PC:admin#config wireless static_ip 10.72.72.110
Command: config wireless static_ip 10.72.72.110

Success.

DWS-3160-24PC:admin#
```

95-28 config wireless trap

Description

This command is used to enable or disable wireless Switch SNMP trap groups for wireless system events.

Format

config wireless trap [enable | disable] [all | ap_failure | ap_state | client_failure | client_state | peer_ws | rf_scan | rogue_ap | wids_status | ws_status]

Parameters

enable - Specifies that the specified Wireless Switch SNMP trap group wireless system event will be enabled.

disable - Specifies that the specified Wireless Switch SNMP trap group wireless system event will be disabled.

all - Specifies that all wireless SNMP traps events will be used.

ap_failure - Specifies the SNMP traps associated with AP association or authentication failures. By default, this option is disabled.

ap_state - Specifies the SNMP traps associated with AP state changes. By default, this option is disabled.

client_failure - Specifies the SNMP traps associated with client association or authentication failures. By default, this option is disabled.

client_state - Specifies the SNMP traps associated with client state changes. By default, this option is disabled.

peer_ws - Specifies the SNMP traps associated with peer Wireless Switch events. By default, this option is disabled.

rf_scan - Specifies the SNMP traps associated with RF scan related events. By default, this option is disabled.

rogue_ap - Specifies the SNMP traps associated with rogue access points. By default, this option is disabled.

wids_status - Specifies the SNMP traps associated with WIDS status events. By default, this option is disabled.

ws_status - Specifies the SNMP traps associated with wireless status events. By default, this option is disabled.

Restrictions

Only Administrators can issue this command.

Example

To enable the wireless AP failure trap:

```
DWS-3160-24PC:admin#config wireless trap enable ap_failure
Command: config wireless trap enable ap_failure

Success.

DWS-3160-24PC:admin#
```

95-29 config wireless tunnel_mtu

Description

This command is used to configure the network MTU size for all access points. This configuration is only used for tunneled networks and is only available if the wireless tunneling feature is enabled. This configuration applies only to the managed access points.

NOTE: The physical ports on the wireless Switch and the rest of the network devices must also be configured with the appropriate MTU size.

Format

config wireless tunnel_mtu [1500 | 1520 | default]

Parameters

1500 - Specifies that the maximum IP frame size is 1518 tagged and 1522 untagged.
1520 - Specifies that the maximum IP frame size is 1538 tagged and 1542 untagged
default - Specifies that the default value will be used. The default value is 1500.

Restrictions

Only Administrators can issue this command.

Example

To configure the tunnel MTU:

```
DWS-3160-24PC:admin#config wireless tunnel_mtu default
Command: config wireless tunnel_mtu default

Warning !! When Tunnel IP MTU Size is changed,
all the clients will be disassociated.
Success.

DWS-3160-24PC:admin#
```

95-30 clear wireless statistics

Description

This command is used to reset the global wireless Switch statistics.

Format

clear wireless statistics

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To reset the global wireless Switch statistics:

```
DWS-3160-24PC:admin#clear wireless statistics
Command: clear wireless statistics

Are you sure you want to clear all wireless statistics? (y/n) y

 Wireless statistics are cleared.

Success.

DWS-3160-24PC:admin#
```

95-31 show wireless

Description

This command is used to display the configured wireless Switch's global parameters and the operational status.

NOTE: The Switch will take several minutes to elect the Cluster Controller.

Format

show wireless

Parameters

None.

Restrictions

None.

Example

To display the wireless Switch's global parameters:

```
DWS-3160-24PC:admin#show wireless
Command: show wireless

----------------------------------------------
*      Wireless Main Status       *
----------------------------------------------
Module Version                       : 4.0.0.1
Administrative Mode                  : Enabled
Operational Status                   : Enabled
WS IP Address                        : 192.168.69.123
WS Auto IP Assign Mode               : Enabled
WS Switch Static IP                  : 10.72.72.110
AP Authentication Mode               : Enabled
AP Auto Upgrade Mode                 : Enabled
AP Validation Method                 : RADIUS
Client Roam Timeout(secs)            : 60
Country Code                         : US - United States
Peer Group ID                        : 168
Cluster Priority                     : 1
Cluster Controller                   : Yes
Cluster Controller IP Address        : 192.168.69.123
Wireless System IP control port      : 57775
AP Client Qos Mode                   : Enabled
Switch Provisioning                  : Enabled
Network Mutual Authentication Mode   : Disabled
Unmanaged AP Re-provisioning Mode    : Enabled
Network Mutual Authentication Status : Not Started
Regenerate X.509 Certificate Status  : Not In Progress

DWS-3160-24PC:admin#
```

95-32 show wireless agetime

Description

This command is used to display the configured age times for the status database entries.

Format

show wireless agetime

Parameters

None.

Display parameters that can be found in the examples:

Ad Hoc Client Statue Age (hours) - Displays how long to continue to display an Ad Hoc client in the status list since it was last detected.

AP Failure Status Age (hours) - Displays how long to continue to display a failed AP in the status list since it was last detected.

RF Scan Status Age (hours) - Displays the clients authenticated to a specific configuration.

Detected Clients Age (hours) - Displays how long to keep an entry in the Detected Client Status list.

AP Provisioning Database Age Time (hours) - Displays the value that determines how long to keep an entry in the AP Provisioning Database. After an AP is inactive for the number of hours you specify in this field, its entry is removed from the database. Range is 0 to 240. If set to 0, entries are not aged-out and remain in the database forever.

Restrictions

None.

Example

To display information of the configured age times for the status database entries:

```
DWS-3160-24PC:admin#show wireless agetime
Command: show wireless agetime

Ad Hoc Client Status Age (hours)              : 20
AP Failure Status Age (hours)                 : 0
RF Scan Status Age (hours)                    : 24
Detected Clients Age (hours)                  : 24
AP Provisioning Database Age Time (hours)     : 72

DWS-3160-24PC:admin#
```

95-33 show wireless ap_capability

Description

This command is used to display AP hardware, image, and dual boot support capabilities.

Format

show wireless ap_capability {[[any | hw_dwl8600 | hw_dwl3600 | hw_dwl6600] radio <int 1-2> | image_table | dual_boot]}

Parameters

any - (Optional) Specifies that a summary of access point hardware type capabilities for all supported AP hardware types is displayed.

hw_dwl8600 - Specifies that detailed hardware type capabilities will be displayed for the DWL-8600.

hw_dwl3600 - Specifies that detailed hardware type capabilities will be displayed for the DWL-3600.

hw_dwl6600 - Specifies that detailed hardware type capabilities will be displayed for the DWL-6600.

radio - (Optional) Specifies the radio index on the AP hardware type. If the selected hardware only supports one radio, Radio 2 displays a message indicating that the radio is invalid for the selected hardware type.

<int 1-2> - Enter the radio index value used here. This value must be between 1 and 2.

image_table - (Optional) Specifies that the AP image capability table will be displayed.

dual_boot - (Optional) Specifies that the AP dual boot support table will be displayed.

Restrictions

None.

Example

To display a summary of access point hardware type capabilities:

```
DWS-3160-24PC:admin#show wireless ap_capability
Command: show wireless ap_capability

Hardware        Hardware                       Radio VAP Count Image
Type            Type Description               Count Per Radio Type
--------------- ------------------------------ ----- --------- ----------------
any             Any                            2     16        img_dwl8600
hw_dwl8600      DWL-8600AP Dual Radio a/b/g/n  2     16        img_dwl8600
hw_dwl3600      DWL-3600AP Single Radio b/g/n  1     16        img_dwl3600-6600
hw_dwl6600      DWL-6600AP Dual Radio a/b/g/n  2     16        img_dwl3600-6600

DWS-3160-24PC:admin#
```

To display the detailed hardware type capability:

```
DWS-3160-24PC:admin#show wireless ap_capability hw_dwl8600 radio 1
Command: show wireless ap_capability hw_dwl8600 radio 1

Hardware Type Description                    : DWL-8600AP Dual Radio a/b/g/n
Radio Count                                  : 2
Image Type                                   : DLink 8600 AP Radios

Radio                                        : 1
Radio Type Description                       : D-Link DWL-8600 a/n
VAP Count                                    : 16
802.11a Support                              : Enable
802.11bg Support                             : Disable
802.11n Support                              : Enable

DWS-3160-24PC:admin#
```

To display the AP image capability table:

```
DWS-3160-24PC:admin#show wireless ap_capability image_table
Command: show wireless ap_capability image_table

Image Type            Image Type Description
--------------------  -------------------------
img_dwl8600           DLink 8600 AP Radios
img_dwl3600-6600      DLink AP-3600/6600 Radios

DWS-3160-24PC:admin#
```

To display the AP dual boot support table:

```
DWS-3160-24PC:admin#show wireless ap_capability dual_boot
Command: show wireless ap_capability dual_boot

Hardware    Hardware                                  Dual Boot
Type ID     Type Description                          Support
----------  ----------------------------------------  -------------
any         Any                                       Not Supported
hw_dwl8600  DWL-8600AP Dual Radio a/b/g/n             Not Supported
hw_dwl3600  DWL-3600AP Single Radio b/g/n             Supported
hw_dwl6600  DWL-6600AP Dual Radio a/b/g/n             Supported

DWS-3160-24PC:admin#
```

95-34 show wireless ap_image availability

Description

This command is used to display the version information of AP images stored on the Switch.

Format

show wireless ap_image availability

Parameters

None.

Restrictions

None.

Example

To display AP image version information:

```
DWS-3160-24PC:admin# show wireless ap_image availability
Command: show wireless ap_image availability

Image Type                 Code Version
----------------  ------------
img_dwl8600         D.9.3.1
img_dwl3600-6600    D.9.8.8

DWS-3160-24PC:admin#
```

95-35 show wireless country_code

Description

This command is used to display the country codes configurable on the wireless Switch.

Format

show wireless country_code

Parameters

None.

Restrictions

None.

Example

To display the country codes configurable on the wireless Switch:

```
DWS-3160-24PC:admin#show wireless country_code
Command: show wireless country_code

 Code  Country
 ----  --------------------------------
 AE    United Arab Emirates
 AG    Antigua and Barbuda
 AN    Netherlands Antilles
 AR    Argentina
 AS    American Samoa
 AT    Austria
 AU    Australia
 AW    Aruba
 AZ    Azerbaijan
 BA    Bosnia
 BB    Barbados
 BD    Bangladesh
 BE    Belgium
 BG    Bulgaria
 BH    Bahrain
 BM    Bermuda
 BN    Brunei
 BO    Bolivia
 BR    Brazil
 BS    Bahamas
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

95-36 show wireless discovery

Description

This command is used to display the configured wireless Switch discovery methods, the configured IP polling list for Layer 3 discovery, and the configured VLAN ID list for Layer 2 discovery.

Format

show wireless discovery {[ip_list | vlan_list]}

Parameters

ip_list - Specifies that the Layer 3 discovery IP list and polling status will be displayed.

vlan_list - Specifies that the Layer 2 discovery VLAN list will be displayed.

If no parameter is specified, information about the configured the wireless Switch's discovery methods will be displayed.

Restrictions

None.

Example

To display information about the configured the wireless Switch's discovery methods:

```
DWS-3160-24PC:admin#show wireless discovery
Command: show wireless discovery

---------------------------------------
*      Wireless Discovery Status      *
---------------------------------------
IP Polling Mode             : Enabled
L2 Multicast Discovery Mode : Enabled

DWS-3160-24PC:admin#
```

To display information about the configured wireless Switch's IP polling list for Layer 3 discovery:

```
DWS-3160-24PC:admin#show wireless discovery ip_list
Command: show wireless discovery ip_list

Maximum Number of Configurable Entries        : 256
Total Number of Configured Entries            : 1
Total Number of Polled Entries                : 1
Total Number of Not-Polled Entries            : 0
Total Number of Discovered Entries            : 0
Total Number of Discovered-Failed Entries     : 0
------------------------------------
*   IP  List                       *
------------------------------------
  IP Address          Status
---------------   ------------------
  10.1.2.3         Polled

Total Entries : 1

DWS-3160-24PC:admin#
```

To display information about the configured VLAN ID list for Layer 2 discovery:

```
DWS-3160-24PC:admin#show wireless discovery vlan_list
Command: show wireless discovery vlan_list

--------------------
*   VLAN List      *
--------------------
  1 - default
  3 - v3

Total Entries : 2

DWS-3160-24PC:admin#
```

95-37 show wireless dist_tunnel

Description

This command is used to display the Layer 2 distributed tunnel's status.

Format

show wireless dist_tunnel {statistics}

Parameters

statistics - (Optional) Specifies to display Layer 2 distributed tunnel statistics.

If no parameter is specified, the Layer 2 distributed tunnel settings will be displayed.

Display parameters that can be found in the examples:

Distributed Tunnel Max Clients - Displays the maximum number of distributed tunneling clients that can roam away from the Home AP at the same time.

Distributed Tunnel Idle Timeout - Displays the number of seconds of no activity by the client before the tunnel to that client is terminated and the client is forced to change its IP address.

Distributed Tunnel Timeout - Displays the number of seconds before the tunnel to the roamed client is terminated and the client is forced to change its IP address.

Distributed Tunnel Max Multicast Replications - Displays the maximum number of tunnels to which a multicast frame is copied on the Home AP.

Distributed Tunnel Packets Transmitted - Displays the total number of packets sent by all APs via distributed tunnels.

Distributed Tunnel Roamed Clients - Displays the total number of clients that successfully roamed away from Home AP using distributed tunneling.

Distributed Tunnel Client Denials - Displays the total number of clients for which the system was unable to set up a distributed tunnel when client roamed.

Restrictions

None.

Example

To display the wireless distributed tunnel's settings:

```
DWS-3160-24PC:admin#show wireless dist_tunnel
Command: show wireless dist_tunnel

 Distributed Tunnel Max Clients                : 800
 Distributed Tunnel Idle Timeout               : 100
 Distributed Tunnel Timeout                    : 300
 Distributed Tunnel Max Multicast Replications : 400

DWS-3160-24PC:admin#
```

To display the wireless distributed tunnel’s statistics:

```
DWS-3160-24PC:admin#show wireless dist_tunnel statistics
Command: show wireless dist_tunnel statistics

 Distributed Tunnel Packets Transmitted : 0
 Distributed Tunnel Roamed Clients      : 0
 Distributed Tunnel Client Denials      : 0


DWS-3160-24PC:admin#
```

95-38 show wireless known_client

Description

This command is used to display the content of the local Known Client database.

Format

show wireless known_client

Parameters

None.

Restrictions

None.

Example

To display the content of the local Known Client database:

```
DWS-3160-24PC:admin#show wireless known_client
Command: show wireless known_client

MAC Address       Name                             Action
----------------- -------------------------------- ----------------
00-18-DE-D7-B4-C1 reception                        deny

Total Entries : 1

DWS-3160-24PC:admin#
```

95-39 show wireless mac_authentication_mode

Description

This command is used to display the configured client MAC authentication mode for the Switch.

If the global MAC Authentication action is configured as “White List”, then any wireless clients with MAC addresses that are specified in the known client list (local or RADIUS), and are not explicitly denied access, are granted access. If a MAC address is not in the list, then access to this client is denied.

If the global MAC Authentication action is configured as “Black List”, then any wireless clients with MAC addresses that are specified in the known client list (local or RADIUS), and are not explicitly granted access, are denied access. If a MAC address is not in the list, then access to this client is granted.

Format

show wireless mac_authentication_mode

Parameters

None.

Restrictions

None.

Example

T o display the configured client MAC authentication mode for the Switch:

```
DWS-3160-24PC:admin#show wireless mac_authentication_mode
Command: show wireless mac_authentication_mode

mac authentication mode                       : black-list

DWS-3160-24PC:admin#
```

95-40 show wireless multicast tx_rates

Description

This command is used to display the multicast transmit rates valid for a specified physical mode. This is intended to help the user to determine valid values for the radio configuration command.

Format

show wireless multicast tx_rates [a | bg]

Parameters

a - Specifies that multicast TX rates of the physical mode, 802.11a, will be displayed.
bg - Specifies that multicast TX rates of the physical mode, 802.11b/g, will be displayed.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To display multicast TX rates of the physical mode, 802.11a:

```
DWS-3160-24PC:admin#show wireless multicast tx_rates a
Command: show wireless multicast tx_rates a

Mode      : 802.11a

Valid Rates (Mbps)
------------------
6 Mbps
9 Mbps
12 Mbps
18 Mbps
24 Mbps
36 Mbps
48 Mbps
54 Mbps

DWS-3160-24PC:admin#
```

To display multicast TX rates of the physical mode, 802.11b/g:

```
DWS-3160-24PC:admin#show wireless multicast tx_rates bg
Command: show wireless multicast tx_rates bg

Mode      : 802.11b/g

Valid Rates (Mbps)
------------------
1 Mbps
2 Mbps
5.5 Mbps
6 Mbps
9 Mbps
11 Mbps
12 Mbps
18 Mbps
24 Mbps
36 Mbps
48 Mbps
54 Mbps

DWS-3160-24PC:admin#
```

95-41 show wireless oui_database

Description

This command is used to display all the OUI entries, created by the Administrator, in the local OUI database.

Format

show wireless oui_database {<ouival>}

Parameters

<ouival> - (Optional) Enter the OUI Value, composed of the higher three octets of the Ethernet MAC address, of the vendor AP or Client here.

If no parameter is specified, then all entries will be displayed.

Restrictions

None.

Example

To display all the OUI entries, created by the Administrator, in the local OUI database:

```
DWS-3160-24PC:admin#show wireless oui_database
Command: show wireless oui_database

OUI Value                      OUI Description
--------------------  --------------------------------
00:00:01              D-Link

Total Entries : 1

DWS-3160-24PC:admin#
```

95-42 show wireless radius

Description

This command is used to display the global RADIUS configuration for wireless clients.

Format

show wireless radius

Parameters

None.

Restrictions

None.

Example

To display the global RADIUS configuration for wireless clients:

```
DWS-3160-24PC:admin#show wireless radius
Command: show wireless radius

RADIUS Accounting                      : Enabled

DWS-3160-24PC:admin#
```

95-43 show wireless rates

Description

This command is used to display the rates valid for a specific physical mode. This is intended to help the user to determine valid values for the radio configuration command.

Format

show wireless rates [a | bg]

Parameters

a - Specifies that TX rates of the physical mode, 802.11a, will be displayed.
bg - Specifies that TX rates of the physical mode, 802.11b/g, will be displayed.

Restrictions

None.

Example

To display TX rates of the physical mode, 802.11a:

```
DWS-3160-24PC:admin#show wireless rates a
Command: show wireless rates a

Mode      : 802.11a

Valid Rates (Mbps)
------------------
6 Mbps
9 Mbps
12 Mbps
18 Mbps
24 Mbps
36 Mbps
48 Mbps
54 Mbps

DWS-3160-24PC:admin#
```

To display TX rates of the physical mode, 802.11b/g:

```
DWS-3160-24PC:admin#show wireless rates bg
Command: show wireless rates bg

Mode      : 802.11b/g

Valid Rates (Mbps)
------------------
1 Mbps
2 Mbps
5.5 Mbps
6 Mbps
9 Mbps
11 Mbps
12 Mbps
18 Mbps
24 Mbps
36 Mbps
48 Mbps
54 Mbps

DWS-3160-24PC:admin#
```

95-44 show wireless statistics

Description

This command is used to display the current global wireless Switch's statistics.

Format

show wireless statistics

Parameters

None.

Restrictions

None.

Example

To display the current global wireless Switch's statistics:

```
DWS-3160-24PC:admin#show wireless statistics
Command: show wireless statistics

 WLAN Bytes Received           : 0
 WLAN Bytes Transmitted        : 0
 WLAN Packets Received         : 0
 WLAN Packets Transmitted      : 0
 WLAN Bytes Receive Dropped    : 0
 WLAN Bytes Transmit Dropped   : 0
 WLAN Packets Receive Dropped  : 0
 WLAN Packets Transmit Dropped : 0


DWS-3160-24PC:admin#
```

95-45 show wireless status

Description

This command is used to display the configured global wireless Switch's status parameters.

Format

show wireless status

Parameters

None.

Restrictions

None.

Example

To display the configured global wireless Switch's status parameters.

```
DWS-3160-24PC:admin#show wireless status
Command: show wireless status

Total Access Points                            : 0
Managed Access Points                          : 0
Connection Failed Access Points                : 0
Discovered Access Points                       : 0
Maximum Managed APs in Peer Group              : 48
Rogue AP Mitigation Count                      : 0
Rogue AP Mitigation Limit                      : 16
Total Clients                                  : 0
Authenticated Clients                          : 0
Maximum Associated Clients                     : 2048
Detected Clients                               : 7
Maximum Detected Clients                       : 4096
Peer Switches                                  : 0
Unknown Access Points                          : 8
Rogue Access Points                            : 2
Standalone Access Points                       : 0
AP Provisioning Count                          : 2
Maximum AP Provisioning Entries                : 96
Distributed Tunnel Clients                     : 0
WLAN Utilization                               : 0 %
Maximum Pre-authentication History Entries     : 500
Total Pre-authentication History Entries       : 0
Maximum Roam History Entries                   : 500
Total Roam History Entries                     : 0

DWS-3160-24PC:admin#
```

95-46 show wireless switch

Description

This command is used to display the wireless Switch's status information.

Format

show wireless switch [<ipaddr> | local] {[statistics | client]}

Parameters

<ipaddr> - Enter the IP address of the wireless Switch, in the wireless system, here.
local - Specifies that local wireless Switch in the wireless system.

statistics - (Optional) Specifies that current wireless Switch statistics will be displayed.

client - (Optional) Specifies to display summarized data for all AP associated client's configuration and status.

Restrictions

None.

Example

To display the local Switch’s summary:

```
DWS-3160-24PC:admin#show wireless switch local
Command: show wireless switch local

Switch IP Address                              : 192.168.69.123
Cluster Priority                               : 1
Total Access Points                            : 0
Managed Access Points                          : 0
Connection Failed Access Points                : 0
Discovered Access Points                       : 0
Maximum Managed Access Points                  : 12
Total Clients                                  : 0
Authenticated Clients                          : 0
Distributed Tunnel Clients                     : 0
WLAN Utilization                               : 0 %

DWS-3160-24PC:admin#
```

To display the local Switch’s statistics:

```
DWS-3160-24PC:admin#show wireless switch local statistics
Command: show wireless switch local statistics

WLAN Bytes Received                            : 0
WLAN Bytes Transmitted                         : 0
WLAN Packets Received                          : 0
WLAN Packets Transmitted                       : 0
WLAN Bytes Receive Dropped                     : 0
WLAN Bytes Transmit Dropped                    : 0
WLAN Packets Receive Dropped                   : 0
WLAN Packets Transmit Dropped                  : 0

DWS-3160-24PC:admin#
```

To display the local Switch’s client information:

```
DWS-3160-24PC:admin# show wireless switch local client
Command: show wireless switch local client

Switch IP Address   Client MAC Address
-----------------  ------------------
50.1.1.61          70-1A-04-3D-F4-C1

Total Entries : 1

DWS-3160-24PC:admin#
```

95-47 show wireless trap

Description

This command is used to display the wireless trap status on the Switch.

Format

show wireless trap

Parameters

None.

Restrictions

None.

Example

To display the wireless trap status on the Switch:

```
DWS-3160-24PC:admin#show wireless trap
Command: show wireless trap

AP Failure Traps           : Enabled
AP State Change Traps      : Disabled
Client Failure Traps       : Disabled
Client State Change Traps  : Disabled
Peer Switch Traps          : Disabled
RF Scan Traps              : Disabled
Rogue AP Traps             : Disabled
WIDS Status Traps          : Disabled
Wireless Status Traps      : Disabled

DWS-3160-24PC:admin#
```

95-48 show wireless tunnel_mtu

Description

This command is used to display the configured network’s MTU size. This is a global configuration for all managed access points.

Format

show wireless tunnel_mtu

Parameters

None.

Restrictions

None.

Example

To display the configured network’s MTU size:

```
DWS-3160-24PC:admin#show wireless tunnel_mtu
Command: show wireless tunnel_mtu

tunnel mtu                                    : 1500

DWS-3160-24PC:admin#
```

Chapter 96 Wireless WIDS AP RF Security Command List

config wireless wids_security admin_config_rogue enable

config wireless wids_security ap_chan_illegal [enable | disable]

config wireless wids_security ap_de_auth_attack [enable | disable]

config wireless wids_security client auth_with_unknown_ap [enable | disable]

config wireless wids_security client configured_auth_rate [enable | disable]

config wireless wids_security client configured_deauth_rate [enable | disable]

config wireless wids_security client configured_probe_rate [enable | disable]

config wireless wids_security client known_client_database [enable | disable]

config wireless wids_security client known_db_location [local | radius_server | default]

config wireless wids_security client max_auth_failure [enable | disable]

config wireless wids_security client oui_database [enable | disable]

config wireless wids_security client rogue_det_trap_interval [0 | <int 60-3600> | default]

config wireless wids_security client threat_mitigation [enable | disable]

config wireless wids_security client threshold_auth_failure [<int 1-99999> | default]

config wireless wids_security client threshold_interval_auth [<int 1-3600> | default]

config wireless wids_security client threshold_interval_deauth [<int 1-3600> | default]

config wireless wids_security client threshold_interval_prob [<int 1-3600> | default]

config wireless wids_security client threshold_value_auth [<int 1-99999> | default]

config wireless wids_security client threshold_value_deauth [<int 1-99999> | default]

config wireless wids_security client threshold_value_prob [<int 1-99999> | default]

config wireless wids_security fakeman_ap_chan_invalid [enable | disable]

config wireless wids_security fakeman_ap_managemed_ssid [enable | disable]

config wireless wids_security fakeman_ap_no_ssid [enable | disable]

config wireless wids_security managed_ap_ssid_invalid [enable | disable]

config wireless wids_security managed_ssid_secu_bad [enable | disable]

config wireless wids_security rogue_det_trap_interval [0 | <int 60-3600> | default]

config wireless wids_security standalone_cfg_invalid [enable | disable]

config wireless wids_security unknown_ap_managed_ssid [enable | disable]

config wireless wids_security unmanaged_ap_wired [enable | disable]

config wireless wids_security wired_detection_interval [<int 0-3600> | default]

show wireless wids_security

show wireless wids_security client

show wireless wids_security client rogue_test_descriptions

show wireless wids_security de_authentication

show wireless wids_security rogue_test_descriptions

96-1 config wireless wids_security admin_config_rogue enable

Description

This command is used to manage Administrator-configured rogue detections or not. If the local database indicates that an AP is rouge, use this variable to report the AP as rogue in the RF Scan.

Format

config wireless wids_security admin_config_rogue enable

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To manage Administrator-configured rogue detections:

```
DWS-3160-24PC:admin#config wireless wids_security admin_config_rogue enable
Command: config wireless wids_security admin_config_rogue enable

Success.

DWS-3160-24PC:admin#
```

96-2 config wireless wids_security ap_chan_illegal

Description

This command is used to manage rogue reporting for APs operating on an illegal channels or not.

Format

config wireless wids_security ap_chan_illegal [enable | disable]

Parameters

enable - Specifies to manage rogue reporting for APs operating on an illegal channels. This is the default option.

disable - Specifies not to manage rogue reporting for APs operating on an illegal channels.

Restrictions

Only Administrators can issue this command.

Example

To enable WIDS security for rogue reporting for APs operating on an illegal channels:

```
DWS-3160-24PC:admin#config wireless wids_security ap_chan_illegal enable
Command: config wireless wids_security ap_chan_illegal enable

Success.

DWS-3160-24PC:admin#
```

96-3 config wireless wids_security ap_de_auth_attack

Description

This command is used to manage an AP de-authentication attack or not.

Format

config wireless wids_security ap_de_auth_attack [enable | disable]

Parameters

enable - Specifies to manage an AP de-authentication attack.

disable - Specifies not to manage an AP de-authentication attack. This is the default option.

Restrictions

Only Administrators can issue this command.

Example

To manage an AP de-authentication attack:

```
DWS-3160-24PC:admin#config wireless wids_security ap_de_auth_attack enable
Command: config wireless wids_security ap_de_auth_attack enable

Success.

DWS-3160-24PC:admin#
```

96-4 config wireless wids_security client auth_with_unknown_ap

Description

This command is used to enable or disable the test to check if a known client is authenticated with an unknown AP. If yes, then the client is marked as a rogue.

Format

config wireless wids_security client auth_with_unknown_ap [enable | disable]

Parameters

enable - Specifies to enable the test to check if a known client is authenticated with an unknown AP.

disable - Specifies to disable the test to check if a known client is authenticated with an unknown AP. This is the default option.

Restrictions

Only Administrators can issue this command.

Example

To enable the test to check if a known client is authenticated with an unknown AP:

```
DWS-3160-24PC:admin#config wireless wids_security client auth_with_unknown_ap
enable
Command: config wireless wids_security client auth_with_unknown_ap enable

Success.

DWS-3160-24PC:admin#
```

96-5 config wireless wids_security client configured_auth_rate

Description

This command is used to enable or disable the test which marks the client as rogue if it exceeds the configured rate for transmitting 802.11 authentication requests.

Format

config wireless wids_security client configured_auth_rate [enable | disable]

Parameters

enable - Specifies to enable the test which marks the client as rogue if it exceeds the configured rate for transmitting 802.11 authentication requests. This is the default option.

disable - Specifies to disable the test which marks the client as rogue if it exceeds the configured rate for transmitting 802.11 authentication requests.

Restrictions

Only Administrators can issue this command.

Example

To enable the test which marks the client as rogue if it exceeds the configured rate for transmitting 802.11 authentication requests:

```
DWS-3160-24PC:admin#config wireless wids_security client configured_auth_rate
enable
Command: config wireless wids_security client configured_auth_rate enable

Success.

DWS-3160-24PC:admin#
```

96-6 config wireless wids_security client configured_deauth_rate

Description

This command is used to enable or disable the test which marks the client as rogue if it exceeds the configured rate for transmitting 802.11 de-authentication requests.

Format

config wireless wids_security client configured_deauth_rate [enable | disable]

Parameters

enable - Specifies to enable the test which marks the client as rogue if it exceeds the configured rate for transmitting 802.11 de-authentication requests. This is the default option.

disable - Specifies to disable the test which marks the client as rogue if it exceeds the configured rate for transmitting 802.11 de-authentication requests.

Restrictions

Only Administrators can issue this command.

Example

To enable the test which marks the client as rogue if it exceeds the configured rate for transmitting 802.11 de-authentication requests:

```
DWS-3160-24PC:admin#config wireless wids_security client configured_deauth_rate
enable
Command: config wireless wids_security client configured_deauth_rate enable

Success.

DWS-3160-24PC:admin#
```

96-7 config wireless wids_security client configured_probe_rate

Description

This command is used to enable or disable the test which marks the client as rogue if it exceeds the configured rate for transmitting probe requests.

Format

config wireless wids_security client configured_probe_rate [enable | disable]

Parameters

enable - Specifies to enable the test which marks the client as rogue if it exceeds the configured rate for transmitting probe requests. This is the default option.

disable - Specifies to disable the test which marks the client as rogue if it exceeds the configured rate for transmitting probe requests.

Restrictions

Only Administrators can issue this command.

Example

To enable the test which marks the client as rogue if it exceeds the configured rate for transmitting probe requests:

```
DWS-3160-24PC:admin#config wireless wids_security client configured_probe_rate
enable
Command: config wireless wids_security client configured_probe_rate enable

Success.

DWS-3160-24PC:admin#
```

96-8 config wireless wids_security client known_client_database

Description

This command is used to enable or disable the test which marks the client as a rogue if it is not in the Known Clients database.

Format

config wireless wids_security client known_client_database [enable | disable]

Parameters

enable - Specifies to enable the test which marks the client as a rogue if it is not in the Known Clients database.

disable - Specifies to disable the test which marks the client as a rogue if it is not in the Known Clients database. This is the default option.

Restrictions

Only Administrators can issue this command.

Example

To enable WIDS security for the known client database:

```
DWS-3160-24PC:admin#config wireless wids_security client known_client_database
enable
Command: config wireless wids_security client known_client_database enable

Success.

DWS-3160-24PC:admin#
```

96-9 config wireless wids_security client known_db_location

Description

This command is used to Specifies the location of the known client database for detected clients.

Format

config wireless wids_security client known_db_location [local | radius_server | default]

Parameters

local - Specifies that the database defined locally. This is the default option.
radius_server - Specifies that the database defined on a RADIUS server.
default - Specifies that the default option will be used.

Restrictions

Only Administrators can issue this command.

Example

To configure the known client database location:

```
DWS-3160-24PC:admin#config wireless wids_security client known_db_location
radius_server
Command: config wireless wids_security client known_db_location radius_server

Success.

DWS-3160-24PC:admin#
```

96-10 config wireless wids_security client max_auth_failure

Description

This command is used to enable or disable the test which marks the client as rogue if it exceeds the maximum number of authentication failures.

Format

config wireless wids_security client max_auth_failure [enable | disable]

Parameters

enable - Specifies to enable the test which marks the client as rogue if it exceeds the maximum number of authentication failures. This is the default option.

disable - Specifies to disable the test which marks the client as rogue if it exceeds the maximum number of authentication failures.

Restrictions

Only Administrators can issue this command.

Example

To enable the test which marks the client as rogue if it exceeds the maximum number of authentication failures:

```
DWS-3160-24PC:admin#config wireless wids_security client max_auth_failure
enable
Command: config wireless wids_security client max_auth_failure enable

Success.

DWS-3160-24PC:admin#
```

96-11 config wireless wids_security client oui_database

Description

This command is used to enable or disable the check whether a client is present in the OUI DB Test.

Format

config wireless wids_security client oui_database [enable | disable]

Parameters

enable - Specifies to enable the check whether a client is present in the OUI DB Test.
disable - Specifies to disable the check whether a client is present in the OUI DB Test.

Restrictions

Only Administrators can issue this command.

Example

To enable or disable the check whether a client is present in the OUI DB Test:

```
DWS-3160-24PC:admin#config wireless wids_security client oui_database enable
Command: config wireless wids_security client oui_database enable

Success.

DWS-3160-24PC:admin#
```

96-12 config wireless wids_security client rogue_det_trap_interval

Description

This command is used to Specifies the interval between transmissions of the trap telling you that rogue clients are present in the detected client database.

Format

config wireless wids_security client rogue_det_trap_interval [0 | <int 60-3600> | default]

Parameters

0 - Specifies that the rogue detection trap interval option will be disabled.
<int 60-3600> - Enter the rogue detection trap interval here. This value must be between 60 and 3600 seconds. The default value is 300 seconds.
default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To configure the rogue detection trap interval:

```
DWS-3160-24PC:admin#config wireless wids_security client
rogue_det_trap_interval 3600
Command: config wireless wids_security client rogue_det_trap_interval 3600

Success.

DWS-3160-24PC:admin#
```

96-13 config wireless wids_security client threat_mitigation

Description

This command is used to enable or disable the transmission of de-authentication messages to known clients associated with unknown APs. The “Known Client” test must also be enabled in order for the mitigation to take place.

Format

config wireless wids_security client threat_mitigation [enable | disable]

Parameters

enable - Specifies to enable the transmission of de-authentication messages to known clients associated with unknown APs.

disable - Specifies to disable the transmission of de-authentication messages to known clients associated with unknown APs. This is the default option.

Restrictions

Only Administrators can issue this command.

Example

To enable the transmission of de-authentication messages to known clients associated with unknown APs:

```
DWS-3160-24PC:admin#config wireless wids_security client threat_mitigation
enable
Command: config wireless wids_security client threat_mitigation enable

Success.

DWS-3160-24PC:admin#
```

96-14 config wireless wids_security client threshold_auth_failure

Description

This command is used to specify the number of 802.1x authentication failures that triggers the client to be reported as rogue.

Format

config wireless wids_security client threshold_auth_failure [<int 1-99999> | default]

Parameters

<int 1-99999> - Enter the threshold authentication failure value used here. This value must be between 1 and 99999. The default value is 5.

default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To Specifies the number of 802.1x authentication failures that triggers the client to be reported as rogue:

```
DWS-3160-24PC:admin#config wireless wids_security client threshold_auth_failure
100
Command: config wireless wids_security client threshold_auth_failure 100

Success.

DWS-3160-24PC:admin#
```

96-15 config wireless wids_security client threshold_interval_auth

Description

This command is used to Specifies the threshold interval for counting the authentication messages at the Switch.

Format

config wireless wids_security client threshold_interval_auth [<int 1-3600> | default]

Parameters

<int 1-3600> - Enter the threshold interval for counting the authentication messages at the Switch here. This value must be between 1 and 3600. The default value is 60.

default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To Specifies the threshold interval for counting the authentication messages at the Switch:

```
DWS-3160-24PC:admin#config wireless wids_security client
threshold_interval_auth 60
Command: config wireless wids_security client threshold_interval_auth 60

Success.

DWS-3160-24PC:admin#
```

96-16 config wireless wids_security client threshold_interval_deauth

Description

This command is used to specify the threshold interval for counting the de-authentication message.

Format

config wireless wids_security client threshold_interval_deauth [<int 1-3600> | default]

Parameters

<int 1-3600> - Enter the threshold interval for counting the de-authentication message here. This value must be between 1 and 3600. The default value is 60.

default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To Specifies the threshold interval for counting the de-authentication message:

```
DWS-3160-24PC:admin#config wireless wids_security client
threshold_interval_deauth 600
Command: config wireless wids_security client threshold_interval_deauth 600

Success.

DWS-3160-24PC:admin#
```

96-17 config wireless wids_security client threshold_interval_prob

Description

This command is used to specify the threshold interval for counting the probe message.

Format

config wireless wids_security client threshold_interval_prob [<int 1-3600> | default]

Parameters

<int 1-3600> - Enter the threshold interval for counting the probe message here. This value must be between 1 and 3600. The default value is 60.

default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To Specifies the threshold interval for counting the probe message:

```
DWS-3160-24PC:admin#config wireless wids_security client
threshold_interval_prob 600
Command: config wireless wids_security client threshold_interval_prob 600

Success.

DWS-3160-24PC:admin#
```

96-18 config wireless wids_security client threshold_value_auth

Description

This command is used to specify the maximum number of authentication messages that a Switch can receive during the threshold interval.

Format

config wireless wids_security client threshold_value_auth [<int 1-99999> | default]

Parameters

<int 1-99999> - Enter the maximum number of authentication messages that a Switch can receive during the threshold interval here. This value must be between 1 and 99999. The default value is 10.

default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To Specifies the maximum number of authentication messages that a Switch can receive during the threshold interval:

```
DWS-3160-24PC:admin#config wireless wids_security client threshold_value_auth
10000
Command: config wireless wids_security client threshold_value_auth 10000

Success.

DWS-3160-24PC:admin#
```

96-19 config wireless wids_security client threshold_value_deauth

Description

This command is used to specify the maximum number of de-authentication messages which a Switch can receive during the threshold interval.

Format

config wireless wids_security client threshold_value_deauth [<int 1-99999> | default]

Parameters

<int 1-99999> - Enter the maximum number of de-authentication messages which a Switch can receive during the threshold interval here. This value must be between 1 and 99999. The default value is 10.

default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To Specifies the maximum number of de-authentication messages which a Switch can receive during the threshold interval:

```
DWS-3160-24PC:admin#config wireless wids_security client threshold_value_deauth
100
Command: config wireless wids_security client threshold_value_deauth 100

Success.

DWS-3160-24PC:admin#
```

96-20 config wireless wids_security client threshold_value_prob

Description

This command is used to specify the maximum number of probe messages that a Switch can receive during the threshold interval.

Format

config wireless wids_security client threshold_value_prob [<int 1-99999> | default]

Parameters

<int 1-99999> - Enter the maximum number of probe messages that a Switch can receive during the threshold interval here. This value must be between 1 and 99999. The default value is 120.

default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To Specifies the maximum number of probe messages that a Switch can receive during the threshold interval:

```
DWS-3160-24PC:admin#config wireless wids_security client threshold_value_prob
100
Command: config wireless wids_security client threshold_value_prob 100

Success.

DWS-3160-24PC:admin#
```

96-21 config wireless wids_security fakeman_ap_chan_invalid

Description

This command is used to manage when a beacon was received from a fake managed AP on an invalid rogue channel or not.

Format

config wireless wids_security fakeman_ap_chan_invalid [enable | disable]

Parameters

enable - Specifies to manage when a beacon was received from a fake managed AP on an invalid rogue channel. This is the default option.

disable - Specifies not to manage when a beacon was received from a fake managed AP on an invalid rogue channel.

Restrictions

Only Administrators can issue this command.

Example

To manage when a beacon was received from a fake managed AP on an invalid rogue channel:

```
DWS-3160-24PC:admin#config wireless wids_security fakeman_ap_chan_invalid
enable
Command: config wireless wids_security fakeman_ap_chan_invalid enable

Success.

DWS-3160-24PC:admin#
```

96-22 config wireless wids_security fakeman_ap_managemed_ssid

Description

This command is used to manage rogue reporting for fake managed AP’s detected with a managed SSID or not.

Format

config wireless wids_security fakeman_ap_managemed_ssid [enable | disable]

Parameters

enable - Specifies to manage rogue reporting for fake managed AP’s detected with a managed SSID. This is the default option.

disable - Specifies not to manage rogue reporting for fake managed AP’s detected with a managed SSID.

Restrictions

Only Administrators can issue this command.

Example

To manage rogue reporting for fake managed AP’s detected with a managed SSID:

```
DWS-3160-24PC:admin#config wireless wids_security fakeman_ap_managemed_ssid
enable
Command: config wireless wids_security fakeman_ap_managemed_ssid enable

Success.

DWS-3160-24PC:admin#
```

96-23 config wireless wids_security fakeman_ap_no_ssid

Description

This command is used to manage beacons received from fake managed AP without SSID rogue detection or not.

Format

config wireless wids_security fakeman_ap_no_ssid [enable | disable]

Parameters

enable - Specifies to manage beacons received from fake managed AP without SSID rogue detection. This is the default option.

disable - Specifies not to manage beacons received from fake managed AP without SSID rogue detection.

Restrictions

Only Administrators can issue this command.

Example

To manage beacons received from fake managed AP without SSID rogue detection:

```
DWS-3160-24PC:admin#config wireless wids_security fakeman_ap_no_ssid enable
Command: config wireless wids_security fakeman_ap_no_ssid enable

Success.

DWS-3160-24PC:admin#
```

96-24 config wireless wids_security managed_ap_ssid_invalid

Description

This command is used to manage invalid SSIDs received from a rogue managed AP or not.

Format

config wireless wids_security managed_ap_ssid_invalid [enable | disable]

Parameters

enable - Specifies to manage invalid SSIDs received from a rogue managed AP. This is the default option.

disable - Specifies not to manage invalid SSIDs received from a rogue managed AP.

Restrictions

Only Administrators can issue this command.

Example

To manage invalid SSIDs received from a rogue managed AP:

```
DWS-3160-24PC:admin#config wireless wids_security managed_ap_ssid_invalid
enable
Command: config wireless wids_security managed_ap_ssid_invalid enable

Success.

DWS-3160-24PC:admin#
```

96-25 config wireless wids_security managed_ssid_secu_bad

Description

This command is used to manage managed SSIDs detected with incorrect security configurations or not.

Format

config wireless wids_security managed_ssid_secu_bad [enable | disable]

Parameters

enable - Specifies to manage managed SSIDs detected with incorrect security configurations. This is the default option.
disable - Specifies to manage managed SSIDs detected with incorrect security configurations.

Restrictions

Only Administrators can issue this command.

Example

To manage managed SSIDs detected with incorrect security configurations:

```
DWS-3160-24PC:admin#config wireless wids_security managed_ssid_secu_bad enable
Command: config wireless wids_security managed_ssid_secu_bad enable

Success.

DWS-3160-24PC:admin#
```

96-26 config wireless wids_security rogue_det_trap_interval

Description

This command is used to Specifies the rogue-detected trap interval. Use this variable to set the interval in seconds between transmissions of the trap telling you that rogues are present in the RF Scan database.

Format

config wireless wids_security rogue_det_trap_interval [0 | <int 60-3600> | default]

Parameters

0 - Specifies to disable the trap from being sent.
<int 60-3600> - Enter the rogue-detected trap interval here, This value must be between 60 and 3600 seconds. This default value is 300 seconds.
default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To configure the rogue-detected trap interval:

```
DWS-3160-24PC:admin#config wireless wids_security rogue_det_trap_interval 3600
Command: config wireless wids_security rogue_det_trap_interval 3600

Success.

DWS-3160-24PC:admin#
```

96-27 config wireless wids_security standalone_cfg_invalid

Description

This command is used to manage standalone APs when operating with an unexpected channel, SSID, security, or WIDS mode or not.

Format

config wireless wids_security standalone_cfg_invalid [enable | disable]

Parameters

enable - Specifies to manage standalone APs when operating with an unexpected channel, SSID, security, or WIDS mode. This is the default option.

disable - Specifies not to manage standalone APs when operating with an unexpected channel, SSID, security, or WIDS mode

Restrictions

Only Administrators can issue this command.

Example

To manage standalone APs when operating with an unexpected channel, SSID, security, or WIDS mode:

```
DWS-3160-24PC:admin#config wireless wids_security standalone_cfg_invalid enable
Command: config wireless wids_security standalone_cfg_invalid enable

Success.

DWS-3160-24PC:admin#
```

96-28 config wireless wids_security unknown_ap_managed_ssid

Description

This command is used to manage managed SSIDs received from unknown rogue APs or not.

Format

config wireless wids_security unknown_ap_managed_ssid [enable | disable]

Parameters

enable - Specifies to manage managed SSIDs received from unknown rogue APs. This is the default option.

disable - Specifies not to manage managed SSIDs received from unknown rogue APs.

Restrictions

Only Administrators can issue this command.

Example

To manage managed SSIDs received from unknown rogue APs:

```
DWS-3160-24PC:admin#config wireless wids_security unknown_ap_managed_ssid
enable
Command: config wireless wids_security unknown_ap_managed_ssid enable

Success.

DWS-3160-24PC:admin#
```

96-29 config wireless wids_security unmanaged_ap_wired

Description

This command is used to manage unmanaged APs that are detected on the wired network or not.

Format

config wireless wids_security unmanaged_ap_wired [enable | disable]

Parameters

enable - Specifies to manage unmanaged APs that are detected on the wired network. This is the default option.

disable - Specifies not to manage unmanaged APs that are detected on the wired network.

Restrictions

Only Administrators can issue this command.

Example

To manage unmanaged APs that are detected on the wired network:

```
DWS-3160-24PC:admin#config wireless wids_security unmanaged_ap_wired enable
Command: config wireless wids_security unmanaged_ap_wired enable

Success.

DWS-3160-24PC:admin#
```

96-30 config wireless wids_security wired_detection_interval

Description

This command is used to specify the minimum wired detection interval. Use this variable to set the minimum number of seconds that the AP waits before starting a new wired network detection cycle.

Format

config wireless wids_security wired_detection_interval [<int 0-3600> | default]

Parameters

<int 0-3600> - Enter the minimum wired detection interval here. This value must be between 0 and 3600 seconds. The default option is 60 seconds. This value 0 means that detection will be disabled.

default - Specifies that the default value will be used.

Restrictions

Only Administrators can issue this command.

Example

To disable the wired detection interval:

```
DWS-3160-24PC:admin#config wireless wids_security wired_detection_interval 0
Command: config wireless wids_security wired_detection_interval 0

Success.

DWS-3160-24PC:admin#
```

96-31 show wireless wids_security

Description

This command is used to display the WIDS security settings and status.

Format

show wireless wids_security

Parameters

None.

Restrictions

None.

Example

To display the WIDS security settings and status:

```
DWS-3160-24PC:admin#show wireless wids_security
Command: show wireless wids_security

Rogue - admin configured Rogue AP's           : Enable
Rogue - AP's on an illegal channel            : Enable
Rogue - fake managed AP / invalid channel     : Enable
Rogue - fake managed AP / no SSID             : Enable
Rogue - managed AP / invalid SSID             : Enable
Rogue - managed SSID / invalid security       : Enable
Rogue - standalone AP / unexpected config     : Enable
Rogue - unknown AP / managed SSID             : Enable
Rogue - fake managed AP / managed SSID        : Enable
Rogue - unmanaged AP on a wired network       : Enable
Rogue detected trap interval                  : 300 seconds
Wired network detection interval              : 60 seconds
AP De-Authentication Attack                   : Disable

DWS-3160-24PC:admin#
```

96-32 show wireless wids_security client

Description

This command is used to display the configured wireless WIDS security settings for a client.

Format

show wireless wids_security client

Parameters

None.

Restrictions

None.

Example

To display the WIDS client security configuration:

```
DWS-3160-24PC:admin#show wireless wids_security client
Command: show wireless wids_security client

Rogue detected trap interval                  : 300 seconds
Rogue-Not in OUI database                     : Disable
Rogue-Not in Known Client list                : Disable
Rogue-Exceeds Auth Req                        : Enable
Rogue-Exceeds DeAuth Req                      : Enable
Rogue-Exceeds Probe Req                       : Enable
Rogue-Exceeds Failed auth                     : Enable
Rogue-Auth with unknown AP                    : Disable
Client Threat Mitigation                      : Disable
De-auth threshold interval                    : 60 seconds
De-auth threshold value                       : 10
Auth threshold interval                       : 60 seconds
Auth threshold value                          : 10
Probe threshold interval                      : 60 seconds
Probe threshold value                         : 120
Auth failure threshold                        : 5
Known DB Location                             : Local

DWS-3160-24PC:admin#
```

96-33 show wireless wids_security client rogue_test_descriptions

Description

This command is used to display to display the WIDS client rogue classification test identifier descriptions.

Format

show wireless wids_security client rogue_test_descriptions

Parameters

None.

Restrictions

None.

Example

To display the WIDS client rogue classification test descriptions:

```
DWS-3160-24PC:admin#show wireless wids_security client rogue_test_descriptions
Command: show wireless wids_security client rogue_test_descriptions

WIDSCLNTROGUE1 :  Known Client Database Test
WIDSCLNTROGUE2 :  Client exceeds configured rate for auth msgs
WIDSCLNTROGUE3 :  Client exceeds configured rate for probe msgs
WIDSCLNTROGUE4 :  Client exceeds configured rate for de-auth msgs
WIDSCLNTROGUE5 :  Client exceeds max failing authentications
WIDSCLNTROGUE6 :  Known client authenticated with unknown AP
WIDSCLNTROGUE7 :  Client OUI not in the OUI Database

DWS-3160-24PC:admin#
```

96-34 show wireless wids_security de_authentication

Description

This command is used to display information about APs against which the Cluster Controller initiated a de-authentication attack.

Format

show wireless wids_security de_authentication

Parameters

None.

Restrictions

None.

Example

To display information about APs against which the Cluster Controller initiated a de-authentication attack:

```
DWS-3160-24PC:admin# show wireless wids_security de_authentication
Command: show wireless wids_security de_authentication

BSSID             Channel Attack Time Age
----------------- ------- ----------- -----------
00-02-BB-00-0A-01 3       0d:00:01:51 0d:00:01:28
00-02-BB-00-14-02 6       0d:00:03:42 0d:00:02:56
00-02-BB-00-1E-03 9       0d:00:05:33 0d:00:04:24
00-02-BB-00-28-04 12      0d:00:07:24 0d:00:05:52

DWS-3160-24PC:admin#
```

96-35 show wireless wids_security rogue_test_descriptions

Description

This command is used to display the WIDS AP rogue classification test identifier descriptions.

Format

show wireless wids_security rogue_test_descriptions

Parameters

None.

Restrictions

None.

Example

To report the status of the WIDS feature:

```
DWS-3160-24PC:admin#show wireless wids_security rogue_test_descriptions
Command: show wireless wids_security rogue_test_descriptions

WIDSAPROGUE01 :  Administrator configured rogue AP
WIDSAPROGUE02 :  Managed SSID from an unknown AP
WIDSAPROGUE03 :  Managed SSID from a fake managed AP
WIDSAPROGUE04 :  AP without an SSID
WIDSAPROGUE05 :  Fake managed AP on an invalid channel
WIDSAPROGUE06 :  Managed SSID detected with incorrect security
WIDSAPROGUE07 :  Invalid SSID from a managed AP
WIDSAPROGUE08 :  AP is operating on an illegal channel
WIDSAPROGUE09 :  Standalone AP with unexpected configuration
WIDSAPROGUE10 :  Unexpected WDS device detected on network
WIDSAPROGUE11 :  Unmanaged AP detected on wired network

DWS-3160-24PC:admin#
```

Chapter 97 Password Recovery Command List

enable password_recovery

disable password_recovery

show password_recovery

97-1 enable password_recovery

Description

This command is used to enable the password recovery mode.

Format

enable password_recovery

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the password recovery mode:

```
DWS-3160-24PC:admin# enable password_recovery
Command: enable password_recovery

Success.

DWS-3160-24PC:admin#
```

97-2 disable password_recovery

Description

This command is used to disable the password recovery mode.

Format

disable password_recovery

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the password recovery mode:

```
DWS-3160-24PC:admin# disable password_recovery
Command: disable password_recovery

Success.

DWS-3160-24PC:admin#
```

97-3 show password_recovery

Description

This command is used to display the password recovery state.

Format

show password_recovery

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display the password recovery state:

```
DWS-3160-24PC:admin#show password_recovery
Command: show password_recovery

 Running Configuration  : Enabled
 NV-RAM Configuration   : Enabled

DWS-3160-24PC:admin#
```

Appendix A Mitigating ARP Spoofing Attacks Using Packet Content ACL

How Address Resolution Protocol works

Address Resolution Protocol (ARP) is the standard method for finding a host's hardware address (MAC address) when only its IP address is known. However, this protocol is vulnerable because crackers can spoof the IP and MAC information in the ARP packets to attack a LAN (known as ARP spoofing). This document is intended to introduce the ARP protocol, ARP spoofing attacks, and the countermeasures brought by D-Link's switches to thwart ARP spoofing attacks.

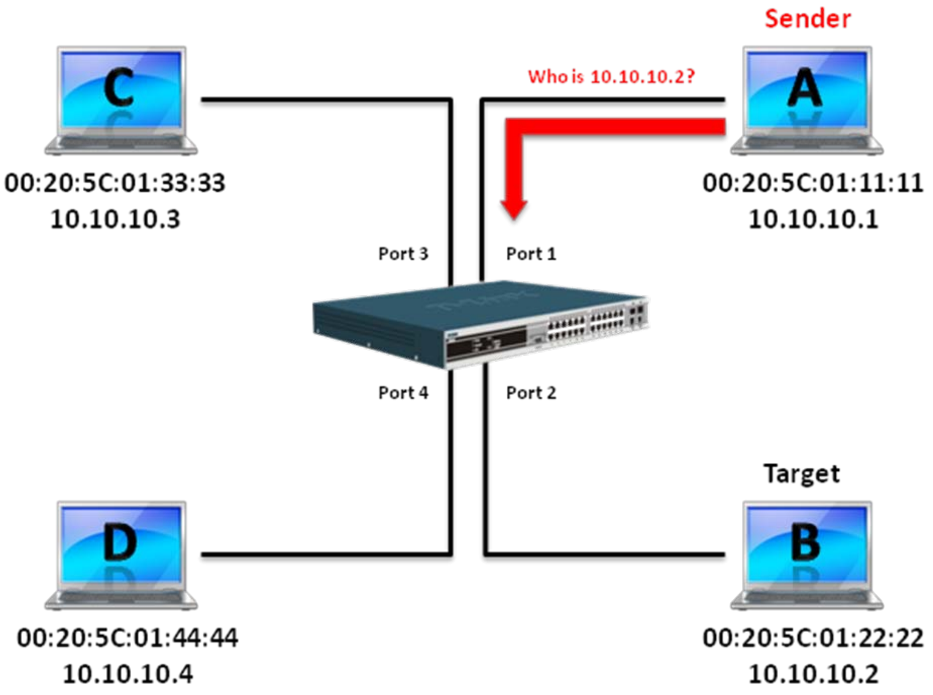


Figure 1

In the process of ARP, PC A will first issue an ARP request to query PC B's MAC address. The network structure is displayed in Figure 1.

In the meantime, PC A's MAC address will be written into the "Sender H/W Address" and its IP address will be written into the "Sender Protocol Address" in the ARP payload. As PC B's MAC address is unknown, the "Target H/W Address" will be "00-00-00-00-00-00," while PC B's IP address will be written into the "Target Protocol Address," displayed in Table1.

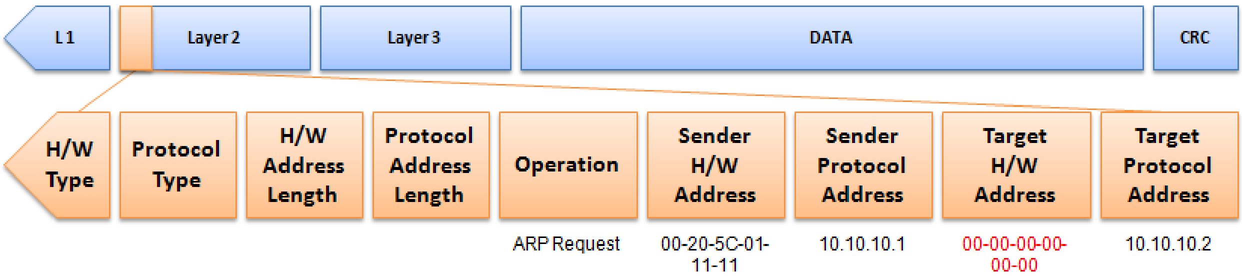


Table 1. ARP Payload

The ARP request will be encapsulated into an Ethernet frame and sent out. As can be seen in Table 2, the “Source Address” in the Ethernet frame will be PC A’s MAC address. Since an ARP request is sent via broadcast, the “Destination address” is in a format of Ethernet broadcast (FF-FF-FF-FF-FF-FF).

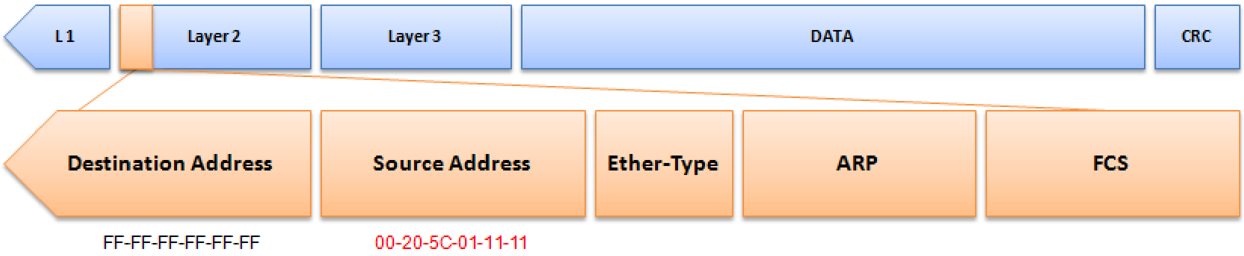


Table 2. Ethernet Frame Format

When the Switch receives the frame, it will check the “Source Address” in the Ethernet frame’s header. If the address is not in its Forwarding Table, the Switch will learn PC A’s MAC and the associated port into its Forwarding Table.

Forwarding Table:
Port 1 : 00-20-5C-01-11-11

In addition, when the Switch receives the broadcasted ARP request, it will flood the frame to all ports except the source port, port 1 (see Figure 2).

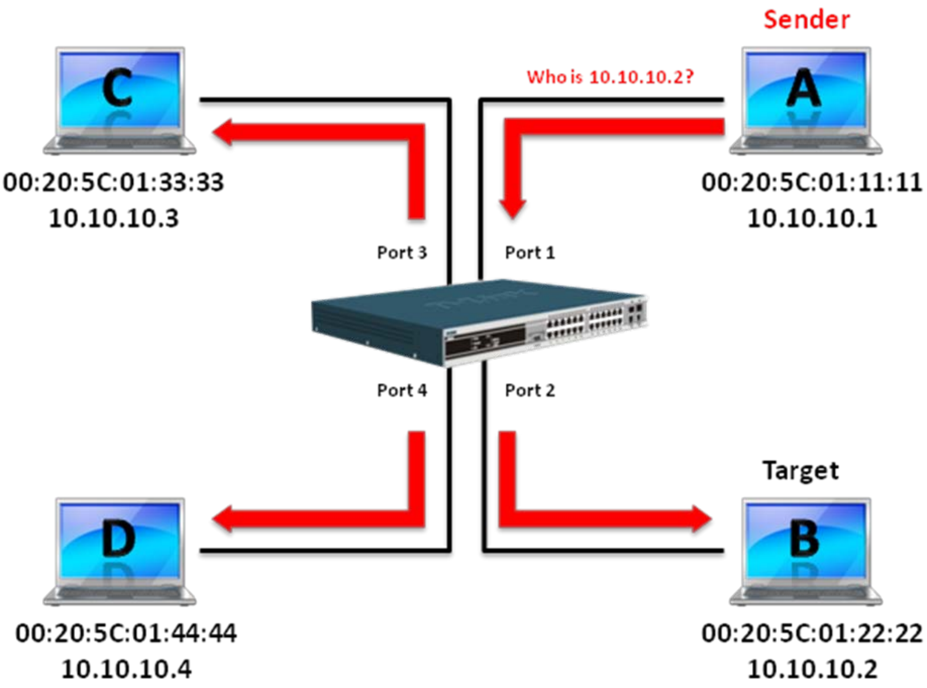


Figure 2

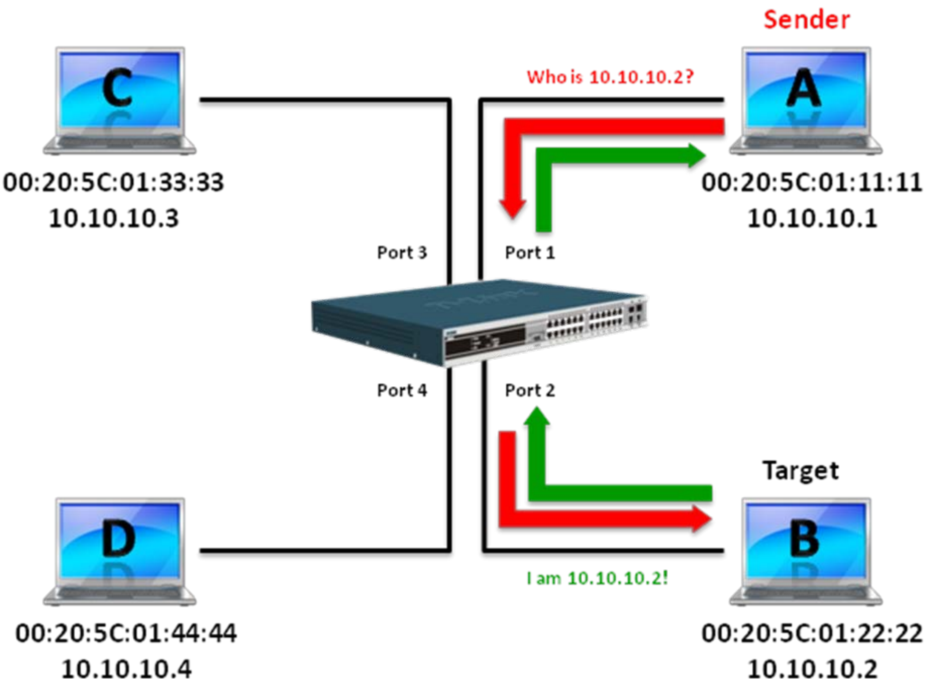


Figure 3

When PC B replies to the ARP request, its MAC address will be written into “Target H/W Address” in the ARP payload displayed in Table 3. The ARP reply will be then encapsulated into an Ethernet frame again and sent back to the sender. The ARP reply is in a form of Unicast communication.

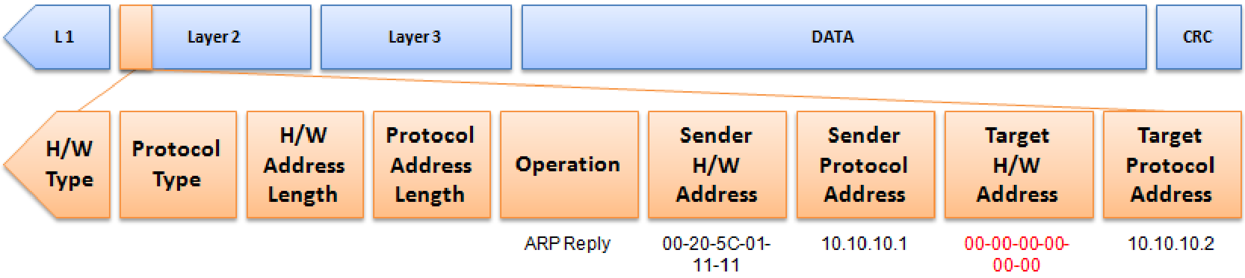


Table 3. ARP Payload

When PC B replies to the query, the “Destination Address” in the Ethernet frame will be changed to PC A’s MAC address. The “Source Address” will be changed to PC B’s MAC address (see Table 4).

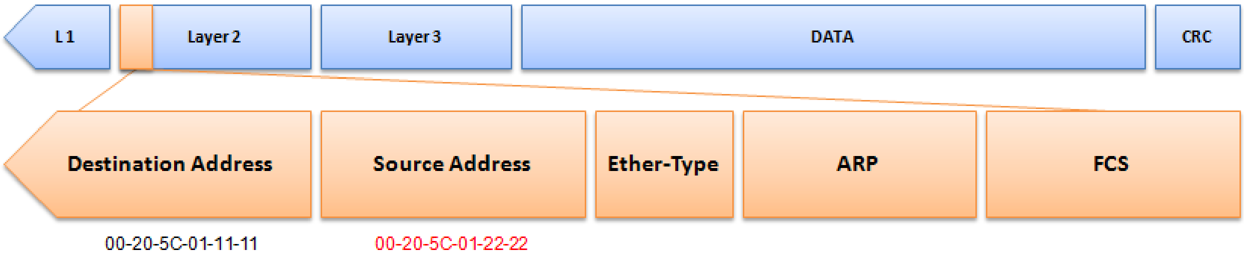


Table 4. Ethernet Frame Format

The Switch will also examine the “Source Address” of the Ethernet frame and find that the address is not in the Forwarding Table. The Switch will learn PC B’s MAC and update its Forwarding Table.

Forwarding Table:
Port 1 : 00-20-5C-01-11-11
Port 2 : 00-20-5C-01-22-22

How ARP Spoofing Attacks a Network

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network which may allow an attacker to sniff data frames on a LAN, modify the traffic, or stop the traffic altogether (known as a Denial of Service – DoS attack). The principle of ARP spoofing is to send the fake, or spoofed ARP messages to an Ethernet network.

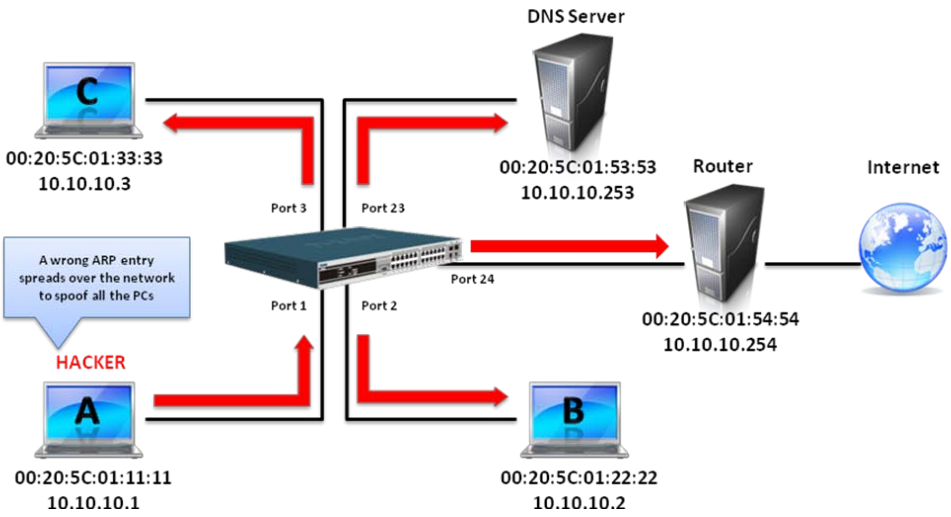
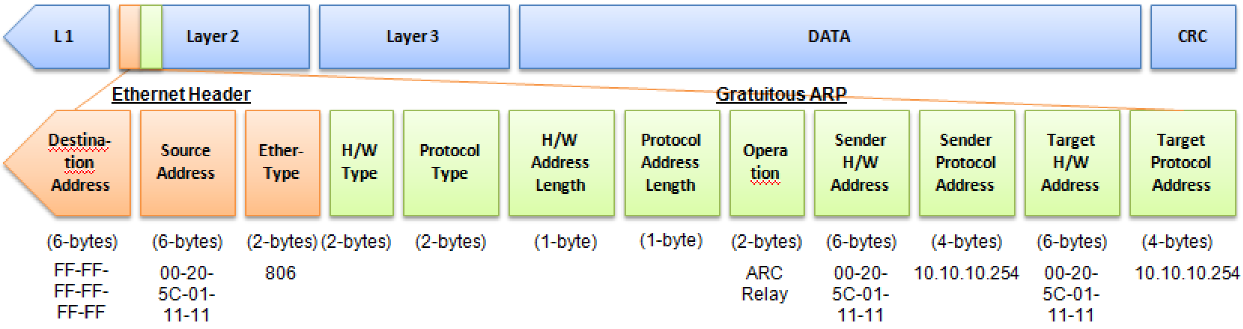


Figure 4

Generally, the aim is to associate the attacker's or random MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

IP spoofing attack is caused by Gratuitous ARP that occurs when a host sends an ARP request to resolve its own IP address. Figure-4 shows a hacker within a LAN to initiate ARP spoofing attack.

In the Gratuitous ARP packet, the “Sender protocol address” and “Target protocol address” are filled with the same source IP address itself. The “Sender H/W Address” and “Target H/W address” are filled with the same source MAC address itself. The destination MAC address is the Ethernet broadcast address (FF-FF-FF-FF-FF-FF). All nodes within the network will immediately update their own ARP table in accordance with the sender’s MAC and IP address. The format of Gratuitous ARP is displayed in the following table.



Destination Address	Source Address	Ether-Type	H/W Type	Protocol Type	H/W Address Length	Protocol Address Length	Operation	Sender H/W Address	Sender Protocol Address	Target H/W Address	Target Protocol Address
(6-bytes)	(6-bytes)	(2-bytes)	(2-bytes)	(2-bytes)	(1-byte)	(1-byte)	(2-bytes)	(6-bytes)	(4-bytes)	(6-bytes)	(4-bytes)
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11	806					ARC Relay	00-20-5C-01-11-11	10.10.10.254	00-20-5C-01-11-11	10.10.10.254

A common DoS attack today can be done by associating a nonexistent or any specified MAC address to the IP address of the network’s default gateway. The malicious attacker only needs to broadcast one Gratuitous ARP to the network claiming it is the gateway so that the whole network operation will be turned down as all packets to the Internet will be directed to the wrong node.

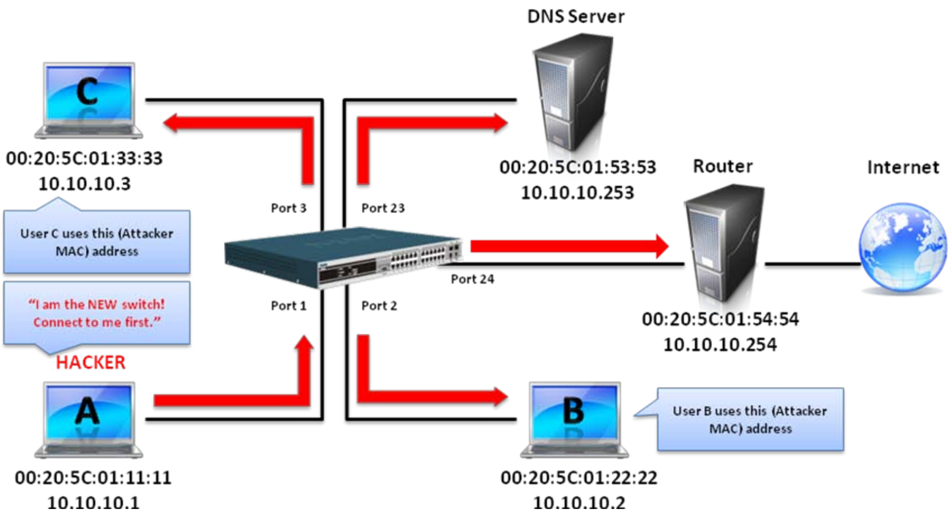


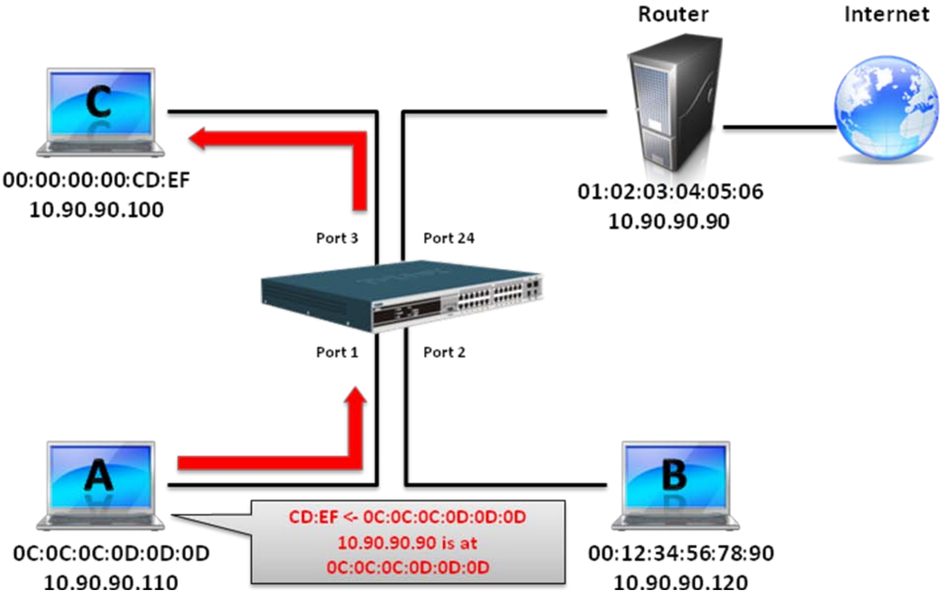
Figure 5

Likewise, the attacker can either choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack).

The hacker cheats the victim PC that it is a router and cheats the router that it is the victim. As can be seen in Figure 5 all traffic will be then sniffed by the hacker but the users will not discover.

Prevent ARP Spoofing via Packet Content ACL

D-Link managed switches can effectively mitigate common DoS attacks caused by ARP spoofing via a unique Package Content ACL.



For the reason that basic ACL can only filter ARP packets based on packet type, VLAN ID, Source, and Destination MAC information, there is a need for further inspections of ARP packets. To prevent ARP spoofing attack, we will demonstrate here via using Packet Content ACL on the Switch to block the invalid ARP packets which contain faked gateway's MAC and IP binding.

Configuration

The configuration logic is as follows:

- Only if the ARP matches Source MAC address in Ethernet, Sender MAC address and Sender IP address in ARP protocol can pass through the Switch. (In this example, it is the gateway's ARP.)
- The Switch will deny all other ARP packets which claim they are from the gateway's IP.

The design of Packet Content ACL on the Switch enables users to inspect any offset chunk. An offset chunk is a 4-byte block in a HEX format, which is utilized to match the individual field in an Ethernet frame. Each profile is allowed to contain up to a maximum of four offset chunks. Furthermore, only one single profile of Packet Content ACL can be supported per Switch. In other words, up to 16 bytes of total offset chunks can be applied to each profile and a Switch. Therefore, a careful consideration is needed for planning and configuration of the valuable offset chunks.

In Table 6, you will notice that the Offset_Chunk0 starts from the 127th byte and ends at the 128th byte. It also can be found that the offset chunk is scratched from 1 but not zero.

Offset Chunk	Offset Chunk0	Offset Chunk1	Offset Chunk2	Offset Chunk3	Offset Chunk4	Offset Chunk5	Offset Chunk6	Offset Chunk7	Offset Chunk8	Offset Chunk9	Offset Chunk10	Offset Chunk11	Offset Chunk12	Offset Chunk13	Offset Chunk14	Offset Chunk15
Byte	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
Byte	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
Byte	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
Byte	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Offset Chunk	Offset Chunk16	Offset Chunk17	Offset Chunk18	Offset Chunk19	Offset Chunk20	Offset Chunk21	Offset Chunk22	Offset Chunk23	Offset Chunk24	Offset Chunk25	Offset Chunk26	Offset Chunk27	Offset Chunk28	Offset Chunk29	Offset Chunk30	Offset Chunk31
Byte	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
Byte	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
Byte	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
Byte	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

Table 6. Chunk and Packet Offset

The following table indicates a completed ARP packet contained in Ethernet frame which is the pattern for the calculation of packet offset.

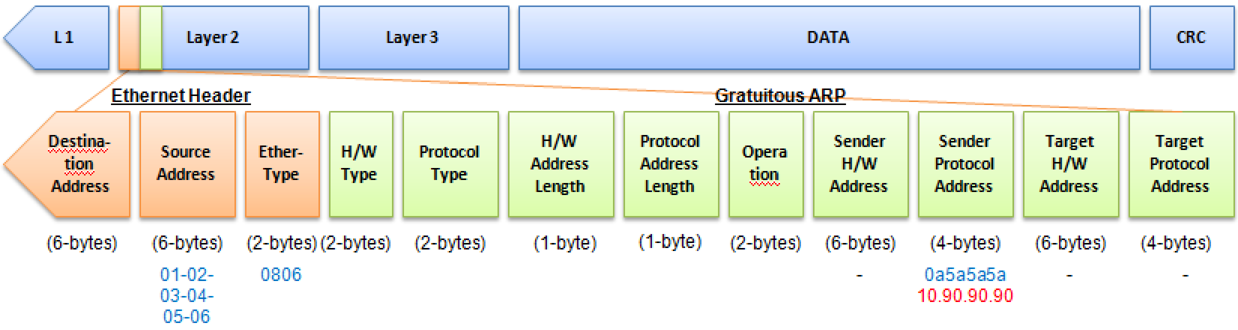


Table 7. A Completed ARP Packet Contained in an Ethernet Frame

	Command	Description
Step 1:	`create access_profile_id 1 profile_name 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type`	1. Create access profile 1 to match Ethernet Type and Source MAC address.
Step 2:	`config access_profile profile_id 1 add access_id 1 ethernet source_mac 01-02-03-04-05-06 ethernet_type 0x806 port 1-12 permit`	2. Configure access profile 1 3. Only if the gateway’s ARP packet that contains the correct Source MAC in the Ethernet frame can pass through the Switch.
Step 3:	`create access_profile profile_id 2 profile_name 2 packet_content_mask offset1 l2 0 0xFF offset2 l2 1 0xFF offset3 l2 16 0xFF offset4 l2 17 0xFF offset5 l2 18 0xFF offset6 l2 19 0xFF`	4. Create access profile 2 5. The first chunk starts from offset 1, 2 mask for Ethernet Type. (Blue in Table 6, 13th and 14th bytes) 6. The second chunk starts from offset 3, 4 mask for Sender IP in ARP packet. (Green in Table 6, 29th and 30th bytes) 7. The third chunk starts from offset 5, 6 mask for Sender IP in ARP packet. (Brown in Table 6, 31st and 32nd bytes)
Step 4:	`config access_profile profile_id 2 add access_id 1 packet_content offset1 l2 0 0x08 offset2 l2 1 0x06 offset3 l2 16 0x0A offset4 l2 17 0x5A offset5 l2 18 0x5A offset6 l2 19 0x5A port 1-12 deny`	8. Configure access profile 2. 9. The rest of the ARP packets whose Sender IP claim they are the gateway’s IP will be dropped.
Step 5:	`save`	10. Save configuration.

Appendix B Password Recovery Procedure

This chapter describes the procedure for resetting passwords on D-Link Switches. Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords get forgotten or destroyed, so network administrators need to reset these passwords. This chapter explains how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

Complete these steps to reset the password:

- For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the Switch.
- Power on the Switch. After the runtime image and UART init are loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [^] (Shift + 6) to enter the “Password Recovery Mode.” Once the Switch enters the “Password Recovery Mode,” all ports on the Switch will be disabled and all port LEDs will be lit.

```
  Boot Procedure                                          V1.00.001
-------------------------------------------------------------------------------


  Power On Self Test ........................................  100 %

  MAC Address   : 00-01-02-03-04-00
  H/W Version   : A1

  Please Wait, Loading V1.00.034 Runtime Image .............  100 %
  UART init .................................................  100 %
```

```
Password Recovery Mode
>
```

- In the “Password Recovery Mode” only the following commands can be used.

Command	Parameters
reset config {force_agree}	The **reset config** command resets the whole configuration back to the default values. If **force_agree** is specified, the configuration will reset to default without the user’s agreement.
reboot	The **reboot** command exits the Reset Password Recovery Mode and restarts the Switch. A confirmation message will be displayed to allow the user to save the current settings.

Command	**Parameters**
reset account	The **reset** account command deletes all the previously created accounts.
reset password {<username>}	The **reset password** command resets the password of the specified user. If a username is not specified, the passwords of all users will be reset.
show account	The **show account** command displays all previously created accounts.

Appendix C System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

Category	Event Description	Log Information	Severity	Remark
System	System started up	**System started up**	Critical	
	System warm start	**System warm start**	Critical	
	System cold start	**System cold start**	Critical	
	Configuration saved to flash	**Configuration saved to flash by console(Username: <username>, IP: <ipaddr>)**	Informational	"by console" and "IP: <ipaddr> " are XOR displayed in log string, which means if user login by console, there will no IP information for logging.
	System log saved to flash	**System log saved to flash by console(Username: <username>, IP: <ipaddr>)**	Informational	"by console" and "IP: <ipaddr> " are XOR displayed in log string, which means if user login by console, there will no IP information for logging.
	Configuration and log saved to flash	**Configuration and log saved to flash by console(Username: <username>, IP: <ipaddr>)**	Informational	"by console" and "IP: <ipaddr> " are XOR displayed in log string, which means if user login by console, there will no IP

				information for logging.
	Internal Power failed	**Internal Power failed**	Critical	
	Internal Power is recovered	**Internal Power is recovered**	Critical	
	Redundant Power failed	**Redundant Power failed**	Critical	
	Redundant Power is working	**Redundant Power is working**	Critical	
	Side Fan failed	**Side Fan failed**	Critical	
	Side Fan recovered	**Side Fan recovered**	Critical	
Upload/Download	Firmware upgraded successfully	**Firmware upgraded by console successfully (Username: <username>, IP: <ipaddr>)**	Informational	"by console" and "IP: <ipaddr>" are XOR displayed in log string, which means if user login by console, there will no IP information for logging.
	Firmware upgrade was unsuccessful	**Firmware upgrade by console was unsuccessful! (Username: <username>, IP: <ipaddr>)**	Warning	"by console" and "IP: <ipaddr>" are XOR displayed in log string, which means if user login by console, there will no IP information for logging.
	Configuration successfully downloaded	**Configuration successfully downloaded by console(Username: <username>, IP: <ipaddr>)**	Informational	"by console" and "IP: <ipaddr>" are XOR displayed in log string, which means if user login by console, there will no IP information for logging.

	Configuration download was unsuccessful	**Configuration download by console was unsuccessful! (Username: <username>, IP: <ipaddr>)**	Warning	"by console" and "IP: <ipaddr> " are XOR displayed in log string, which means if user login by console, there will no IP information for logging.
	Configuration successfully uploaded	**Configuration successfully uploaded by console (Username: <username>, IP: <ipaddr>)**	Informational	"by console" and "IP: <ipaddr> " are XOR displayed in log string, which means if user login by console, there will no IP information for logging.
	Configuration upload was unsuccessful	**Configuration upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)**	Warning	"by console" and "IP: <ipaddr> " are XOR displayed in log string, which means if user login by console, there will no IP information for logging.
	Log message successfully uploaded	**Log message successfully uploaded by console (Username: <username>, IP: <ipaddr>)**	Informational	"by console" and "IP: <ipaddr> " are XOR displayed in log string, which means if user login by console, there will no IP informati

				on for logging.
	Log message upload was unsuccessful	**Log message upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)**	Warning	"by console" and "IP: <ipaddr>" are XOR displayed in log string, which means if user login by console, there will no IP information for logging.
	Firmware successfully uploaded	**Firmware successfully uploaded by console (Username: <username>, IP: <ipaddr>)**	Informational	"by console" and "IP: <ipaddr>" are XOR displayed in log string, which means if user login by console, there will no IP information for logging.
	Firmware upload was unsuccessful	**Firmware upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)**	Warning	"by console" and "IP: <ipaddr>" are XOR displayed in log string, which means if user login by console, there will no IP information for logging.
Interface	Port link up	**Port <portNum> link up, <link state>**	Informational	link state, for ex: , 100Mbps FULL duplex
	Port link down	**Port <portNum> link down**	Informational	
Console	Successful login through Console	**Successful login through Console (Username: <username>)**	Informational	There are no IP and MAC if login by console.

	Login failed through Console	**Login failed through Console (Username: <username>)**	Warning	There are no IP and MAC if login by console.
	Logout through Console	**Logout through Console (Username: <username>)**	Informational	There are no IP and MAC if login by console.
	Console session timed out	**Console session timed out (Username: <username>)**	Informational	There are no IP and MAC if login by console.
Web	Successful login through Web	**Successful login through Web (Username: <username>, IP: <ipaddr>)**	Informational	
	Login failed through Web	**Login failed through Web (Username: <username>, IP: <ipaddr>)**	Warning	
	Logout through Web	**Logout through Web (Username: <username>, IP: <ipaddr>)**	Informational	
	Web session timed out	**Web session timed out (Username: <username>, IP: <ipaddr>)**	Informational	
	Successful login through Web(SSL)	**Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>)**	Informational	
	Login failed through Web(SSL)	**Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>)**	Warning	
	Logout through Web(SSL)	**Logout through Web(SSL) (Username: <username>, IP: <ipaddr>)**	Informational	
	Web(SSL) session timed out	**Web(SSL) session timed out (Username: <username>, IP: <ipaddr>)**	Informational	
TELNET	Successful login through TELNET	**Successful login through TELNET (Username: <username>, IP: <ipaddr>)**	Informational	
	Login failed through TELNET	**Login failed through TELNET (Username: <username>, IP: <ipaddr>)**	Warning	
	Logout through TELNET	**Logout through TELNET (Username: <username>, IP: <ipaddr>)**	Informational	
	TELNET session timed out	**TELNET session timed out (Username: <username>, IP: <ipaddr>)**	Informational	
SNMP	SNMP request received with invalid community string	**SNMP request received from <ipAddress> with invalid community string!**	Informational	
STP	Topology changed	**Topology changed (Instance:<InstanceID> ,Port:<portNum >,MAC:<macaddr>)**	Informational	
	New Root selected	**[CIST | CIST Regional | MSTI Regional] New Root bridge selected([Instance: <InstanceID>]MAC: <macaddr> Priority :<value>)**	Informational	
	Spanning Tree Protocol is enabled	**Spanning Tree Protocol is enabled**	Informational	
	Spanning Tree Protocol is disabled	**Spanning Tree Protocol is disabled**	Informational	
	New root port	**New root port selected (Instance:<InstanceID>, port:<portNum>)**	Notice	
	Spanning Tree port status changed	**Spanning Tree port status change (Instance:<InstanceID> , Port:<portNum>) <old_status> -> <new_status>**	Notice	
	Spanning Tree port role changed	**Spanning Tree port role change (Instance:<InstanceID> , Port:<portNum>) <old_role> -> <new_role>**	Informational	
	Spanning Tree instance	**Spanning Tree instance created**	Informational	

	created	**(Instance:<InstanceID>)**		
	Spanning Tree instance deleted	**Spanning Tree instance deleted (Instance:<InstanceID>)**	Informational	
	Spanning Tree Version changed	**Spanning Tree version change (new version:<new_version>)**	Informational	
	Spanning Tree MST configuration ID name and revision level changed	**Spanning Tree MST configuration ID name and revision level change (name:<name> ,revision level <revision_level>).**	Informational	
	Spanning Tree MST configuration ID VLAN mapping table deleted	**Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>])**	Informational	
	Spanning Tree MST configuration ID VLAN mapping table added	**Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>])**	Informational	
DoS	Spoofing attack 1. The source IP is same as Switch's interface IP but the source MAC is different 2. Source IP is the same as the Switch's IP in ARP packet 3. Self IP packet detected	**Possible spoofing attack from IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>**	Critical	
SSH	Successful login through SSH	**Successful login through SSH (Username: <username>, IP: <ipaddr>)**	Informational	
	Login failed through SSH	**Login failed through SSH (Username: <username>, IP: <ipaddr>,)**	Warning	
	Logout through SSH	**Logout through SSH (Username: <username>, IP: <ipaddr>)**	Informational	
	SSH session timed out	**SSH session timed out (Username: <username>, IP: <ipaddr>)**	Informational	
	SSH server is enabled	**SSH server is enabled**	Informational	
	SSH server is disabled	**SSH server is disabled**	Informational	
AAA	Authentication Policy is enabled	**Authentication Policy is enabled (Module: AAA)**	Informational	
	Authentication Policy is disabled	**Authentication Policy is disabled (Module: AAA)**	Informational	
	Successful login through Console authenticated by AAA local method	**Successful login through Console authenticated by AAA local method (Username: <username>)**	Informational	
	Login failed through Console authenticated by AAA local method	**Login failed through Console authenticated by AAA local method (Username: <username>)**	Warning	
	Successful login through Web authenticated by AAA local method	**Successful login through Web from <userIP> authenticated by AAA local method (Username: <username>)**	Informational	
	Login failed through Web authenticated by AAA local method	**Login failed failed through Web from <userIP> authenticated by AAA local method (Username: <username>)**	Warning	
	Successful login through Web(SSL) authenticated by AAA local method	**Successful login through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>)**	Informational	
	Login failed through Web(SSL) authenticated by AAA local method	**Login failed through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>)**	Warning	
	Successful login through TELNET authenticated by AAA local method	**Successful login through TELNET from <userIP> authenticated by AAA local method (Username: <username>,)**	Informational	
	Login failed through TELNET authenticated by AAA local method	**Login failed through TELNET from <userIP> authenticated by AAA local method (Username: <username>)**	Warning	
	Successful login through SSH authenticated by	**Successful login through SSH from <userIP> authenticated by AAA local**	Informational	

	AAA local method	**method (Username: <username>)**		
	Login failed through SSH authenticated by AAA local method	**Login failed through SSH from <userIP> authenticated by AAA local method (Username: <username>)**	Warning	
	Successful login through Console authenticated by AAA none method	**Successful login through Console authenticated by AAA none method (Username: <username>)**	Informational	
	Successful login through Web authenticated by AAA none method	**Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful login through Web(SSL) authenticated by AAA none method	**Successful login through Web(SSL) from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful login through TELNET authenticated by AAA none method	**Successful login through TELNET from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful login through SSH authenticated by AAA none method	**Successful login through SSH from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful login through Console authenticated by AAA server	**Successful login through Console authenticated by AAA server <serverIP> (Username: <username>)**	Informational	There are no IP and MAC if login by console.
	Login failed through Console authenticated by AAA server	**Login failed through Console authenticated by AAA server <serverIP> (Username: <username>)**	Warning	There are no IP and MAC if login by console.
	Login failed through Console due to AAA server timeout or improper configuration	**Login failed through Console due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful login through Web authenticated by AAA server	**Successful login through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Login failed through Web authenticated by AAA server	**Login failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Login failed through Web due to AAA server timeout or improper configuration	**Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful login through Web(SSL) authenticated by AAA server	**Successful login through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Login failed through Web(SSL) authenticated by AAA server	**Login failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Login failed through Web(SSL) due to AAA server timeout or improper configuration	**Login failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful login through TELNET authenticated by AAA server	**Successful login through TELNET from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Login failed through TELNET authenticated by AAA server	**Login failed through TELNET from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Login failed through TELNET due to AAA server timeout or improper configuration	**Login failed through TELNET from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	

	Successful login through SSH authenticated by AAA server	**Successful login through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Login failed through SSH authenticated by AAA server	**Login failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Login failed through SSH due to AAA server timeout or improper configuration	**Login failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful Enable Admin through Console authenticated by AAA local_enable method	**Successful Enable Admin through Console authenticated by AAA local_enable method (Username: <username>)**	Informational	
	Enable Admin failed through Console authenticated by AAA local_enable method	**Enable Admin failed through Console authenticated by AAA local_enable method (Username: <username>)**	Warning	
	Successful Enable Admin through Web authenticated by AAA local_enable method	**Successful Enable Admin through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Informational	
	Enable Admin failed through Web authenticated by AAA local_enable method	**Enable Admin failed through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Warning	
	Successful Enable Admin through Web(SSL) authenticated by AAA local_enable method	**Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>,)**	Informational	
	Enable Admin failed through Web(SSL) authenticated by AAA local_enable method	**Enable Admin failed through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Warning	
	Successful Enable Admin through TELNET authenticated by AAA local_enable method	**Successful Enable Admin through TELNET from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Informational	
	Enable Admin failed through TELNET authenticated by AAA local_enable method	**Enable Admin failed through TELNET from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Warning	
	Successful Enable Admin through SSH authenticated by AAA local_enable method	**Successful Enable Admin through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Informational	
	Enable Admin failed through SSH authenticated by AAA local_enable method	**Enable Admin failed through <TELNET or Web or SSH> from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Warning	
	Successful Enable Admin through Console authenticated by AAA none method	**Successful Enable Admin through Console authenticated by AAA none method (Username: <username>)**	Informational	
	Successful Enable Admin through Web authenticated by AAA none method	**Successful Enable Admin through Web from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful Enable Admin through Web(SSL) authenticated by AAA none method	**Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful Enable Admin through TELNET authenticated by AAA none method	**Successful Enable Admin through TELNET from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful Enable Admin through SSH authenticated by AAA none method	**Successful Enable Admin through SSH from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	

	Successful Enable Admin through Console authenticated by AAA server	**Successful Enable Admin through Console authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through Console authenticated by AAA server	**Enable Admin failed through Console authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Enable Admin failed through Console due to AAA server timeout or improper configuration	**Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful Enable Admin through Web authenticated by AAA server	**Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through Web authenticated by AAA server	**Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Enable Admin failed through Web due to AAA server timeout or improper configuration	**Enable Admin failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful Enable Admin through Web(SSL) authenticated by AAA server	**Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through Web(SSL) authenticated by AAA server	**Enable Admin failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Enable Admin failed through Web(SSL) due to AAA server timeout or improper configuration	**Enable Admin failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful Enable Admin through TELNET authenticated by AAA server	**Successful Enable Admin through TELNET from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through TELNET authenticated by AAA server	**Enable Admin failed through TELNET from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Enable Admin failed through TELNET due to AAA server timeout or improper configuration	**Enable Admin failed through TELNET from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful Enable Admin through SSH authenticated by AAA server	**Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through SSH authenticated by AAA server	**Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Enable Admin failed through SSH due to AAA server timeout or improper configuration	**Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
Port Security	port security is exceeded to its maximum learning size and will not learn any new address	**Port security violation (MAC address: <macaddr> on port: <portNum>)**	Warning	
MBAC	A host fails to pass the authentication	**MAC-based Access Control unauthenticated host(MAC: <macaddr>, Port <portNum>, VID: <vid>)**	Critical	
	The authorized user number on a port reaches	**Port <portNum> enters MAC-based Access Control stop learning state.**	Warning	per port

	the max user limit.			
	The authorized user number on a port is below the max user limit in a time interval	**Port <portNum> recovers from MAC-based Access Control stop learning state.**	Warning	per port
	The authorized user number on whole device reaches the max user limit.	**MAC-based Access Control enters stop learning state.**	Warning	per system
	The authorized user number on whole device is below the max user limit in a time interval	**MAC-based Access Control recovers from stop learning state.**	Warning	per system
	A host passes the authentication	**MAC-based Access Control host login successful (MAC: <macaddr>, port: <portNum>, VID: <vid>)**	Informational	
	A host is aged out	**MAC-based Access Control host aged out (MAC: <macaddr>, port: <portNum>, VID: <vid>)**	Informational	
IMPB	Unauthenticated IP address encountered and discarded by IP IP-MAC port binding	**Unauthenticated IP-MAC address and discarded by IMPB (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)**	Warning	
	Dynamic IMPB entry is conflict with static ARP	**Dynamic IMPB entry conflicts with static ARP(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)**	Warning	
	Dynamic IMPB entry is conflict with static FDB	**Dynamic IMPB entry conflicts with static FDB(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)**	Warning	
	Dynamic IMPB entry conflicts with static IMPB	**Dynamic IMPB entry conflicts with static IMPB(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)**	Warning	
	Creating IMPB entry failed due to no ACL rule available	**Creating IMPB entry failed due to no ACL rule being available(IP:<ipaddr>, MAC: <macaddr>, Port <portNum>)**	Warning	
IP and Password Changed	IP Address change activity	**Management IP address was changed by console(Username: <username>,IP:<ipaddr>)**	Informational	"console" and "IP: <ipaddr>" are XOR displayed in log string, which means if user login by console, there will no IP information for logging.
	Password change activity	**Password was changed by console (Username: <username>,IP:<ipaddr>)**	Informational	"console" and "IP: <ipaddr>" are XOR displayed in log string, which means if user login by console, there will no IP information for

				logging.
Safeguard Engine	Safeguard Engine is in normal mode	**Safeguard Engine enters NORMAL mode**	Informational	
	Safeguard Engine is in filtering packet mode	**Safeguard Engine enters EXHAUSTED mode**	Warning	
Packet Storm	Broadcast storm occurrence	**Port <portNum> Broadcast storm is occurring**	Warning	
	Broadcast storm cleared	**Port <portNum> Broadcast storm has cleared**	Informational	
	Multicast storm occurrence	**Port <portNum> Multicast storm is occurring**	Warning	
	Multicast storm cleared	**Port <portNum> Multicast storm has cleared**	Informational	
	Port shut down due to a packet storm	**Port <portNum> is currently shut down due to a packet storm**	Warning	
Loopback Dection	Port loop occurred	**Port <portNum> LBD loop occurred. Port blocked**	Critical	
	Port loop detection restarted after interval time	**Port <portNum> LBD port recovered. Loop detection restarted**	Informational	
	Port with VID loop occurred	**Port <portNum> VID <vlanID> LBD loop occurred. Packet discard begun**	Critical	
	Port with VID Loop detection restarted after interval time	**Port <portNum> VID <vlanID> LBD recovered. Loop detection restarted**	Informational	
	The number of VLANs that loop back has occurred hit the specified number.	**Loop VLAN number overflow**	Informational	
Gratuitous ARP	Gratuitous ARP detected duplicate IP.	**Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>, Interface: <ipif_name>).**	Warning	
DHCP	Detect untrusted DHCP server IP address	**Detected untrusted DHCP server(IP: <ipaddr>, Port: <portNum>)**	Informational	DHCP Server Screening
BPDU Protection	BPDU attack happened	**Port <portNum> enter BPDU under attacking state (mode: drop / block / shutdown)**	Informational	
	BPDU attack automatically recover	**Port <portNum> recover from BPDU under attacking state automatically**	Informational	
	BPDU attack manually recover	**Port <portNum> recover from BPDU under attacking state manually**	Informational	
Monitor	Temperature exceeds confidence level	**Temperature Sensor <sensorID> enter alarm state. (current temperature: <temperature>)**	Warning	
	Temperature recovers to normal.	**Temperature Sensor <sensorID> recovers to normal state. (current temperature: <temperature>)**	Informational	
CFM	Cross-connect is detected	**CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Port <portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)**	Critical	
	Error CFM CCM packet is detected	**CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)**	Warning	
	Can not receive remote MEP's CCM packet	**CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>)**	Warning	
	Remote MEP's MAC reports an error status	**CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>,**	Warning	

		Local(Port <portNum>, Direction:<mepdirection>)		
	Remote MEP detects CFM defects	**CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>)**	Informational	
CFM Extension	AIS condition detected	**AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>)**	Notice	
	AIS condition cleared	**AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>)**	Notice	
	LCK condition detected	**LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>)**	Notice	
	LCK condition cleared	**LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>)**	Notice	
Voice VLAN	When a new voice device is detected in the port	**New voice device detected (MAC:<macaddr>,Port:<portNum>)**	Informational	
	While the port join to the voice VLAN while the port is auto voice VLAN mode	**Port <portNum> add into voice VLAN <vid >**	Informational	
	While the port withdraws from the voice VLAN while there is no more voice device detected in the aging interval.	**Port <portNum> remove from voice VLAN <vid >**	Informational	
ERPS	Signal failure detected	**Signal failure detected on node <macaddr>**	Notice	
	Signal failure cleared	**Signal failure cleared on node <macaddr>**	Notice	
	RPL owner conflict	**RPL owner conflicted on the ring <macaddr>**	Warning	
Command logging	Command Logging	**<username>: execute command "<string>".**	Informational	
Wireless State	Wireless Switch enabled	**Wireless switch enabled**	Informational	
	Wireless Switch disabled	**Wireless switch disabled**	Informational	
	Wireless locally managed AP limit is exceeded	**Wireless Local Managed AP Exceeded MAC: <macaddr>**	Warning	
	Wireless AP Hardware Type unsupported	**Wireless AP Hardware Type Failure MAC: <macaddr> Hardware Type: <int>**	Warning	
Table Full	Wireless managed AP database full	**Wireless managed AP database full AP MAC: <macaddr> dropped**	Warning	
	Wireless managed AP-AP neighbor list full	**Wireless managed AP-AP neighbor list full**	Warning	
	Wireless managed AP-Client neighbor list full	**Wireless managed AP-Client neighbor list full**	Warning	
	Wireless AP failure list full	**Wireless AP failure list full**	Warning	
	Wireless RF scan AP list full	**Wireless RF scan AP list full**	Warning	
	Wireless client association database full	**Wireless client association database full client MAC: <macaddr> dropped**	Warning	
	Wireless Ad Hoc client list full	**Wireless Ad Hoc client list full**	Warning	
	Wireless peer Switch managed AP database full	**Wireless peer switch <ipaddr> managed AP database full AP MAC: <macaddr>**	Warning	

		dropped		
	Wireless peer Switch client database full	**Wireless peer switch <ipaddr> client database full client MAC: <macaddr> dropped**	Warning	
Peer Switch	Wireless peer Switch discovered	**Wireless peer switch: <ipaddr> discovered**	Informational	
	Wireless peer Switch failed	**Wireless peer switch: <ipaddr> failed**	Warning	
	Wireless peer Switch protocol version unknown	**Wireless peer switch: <ipaddr> protocol version: <version> unknown**	Warning	
	Wireless peer switch Managed AP database limit has exceeded	**Wireless peer switch <ipaddr> managed AP database full AP MAC: <macaddr> dropped**	Warning	
Managed AP	Wireless managed AP discovered	**Wireless managed AP MAC: <macaddr> discovered**	Informational	
	Wireless managed AP failed	**Wireless managed AP MAC: <macaddr> failed**	Warning	
	Wireless managed AP protocol version unknown	**Wireless managed AP MAC: <macaddr> protocol version:<string> unknown**	Warning	
	Wireless managed AP Association failed	**Wireless managed AP MAC: <macaddr> Association failed**	Warning	
	Wireless managed AP Authentication failed	**Wireless managed AP MAC: <macaddr> Authentication failed**	Warning	
RF Scan	Wireless RF scan rogue-AP detected	**Wireless RF scan rogue-AP MAC: <macaddr> AP MAC: <macaddr> Radio If: <int> SSID: <ssid> detected**	Informational	
	Wireless RF scan new Neighbor AP detected	**Wireless RF scan new Neighbor AP MAC: <macaddr> AP MAC: <macaddr> Radio If: <int> SSID: <ssid> detected**	Informational	
	Wireless RF scan new Client detected	**Wireless RF scan new Client MAC: <macaddr> AP MAC: <macaddr> Radio If: <int> detected**	Informational	
	Wireless Client Association detected	**Wireless Client Association MAC: <macaddr> VAP MAC: <macaddr> AP MAC: <macaddr> SSID: <ssid> Security Mode: <string> detected**	Informational	
	Wireless Client Disassociation detected	**Wireless Client Disassociation MAC: <macaddr> VAP MAC: <macaddr>AP MAC: <macaddr> detected**	Informational	
	Wireless Client Roam detected	**Wireless Client Roam MAC: <macaddr> VAP MAC: <macaddr> AP MAC: <macaddr>detected**	Informational	
	Wireless Client Association Failure detected	**Wireless Client MAC: <macaddr> Association Failure detected**	Warning	
	Wireless Client Authentication Failure detected	**Wireless Client MAC: <macaddr> Authentication Failure detected**	Warning	
	Wireless RF scan new Ad-Hoc Client detected	**Wireless RF scan new Ad-Hoc Client MAC: <macaddr> AP MAC: <macaddr> Radio If: <int> detected**	Informational	
Load Balacing	Wireless load balancing utilization overflow	**Wireless load balancing utilization overflow: AP MAC: <macaddr> Radio If: <int> Radio MAC: <macaddr> Utilization: <int>**	Warning	
Configuration Push	Wireless peer Switch config push command received	**Wireless peer switch config push command with mask <int> from switch: <ipaddr> received**	Informational	
WIDS	Local Switch is elected as WIDS Controller	**Local Switch is elected as WIDS Controller**	Informational	
	Wireless Network Managed AP Max AP exceeded on WIDS Controller	**Wireless Network Managed AP Max AP exceeded on WIDS Controller <ipaddr> when AP MAC: <macaddr> with IP address <ipaddr> connected to Wireless Switch <ipaddr>**	Warning	
	Wireless rogue-AP(s) present in the network	**Wireless rogue-AP(s) present in the network**	Informational	
	Wireless Detected client list full	**Wireless Detected client list full**	Warning	

	Wireless rogue-Client(s) present in the network	**Wireless rogue-Client(s) present in the network**	Informational	
Auto Channel & Power	Wireless Channel Algorithm is complete	**Wireless Channel Algorithm is complete**	Informational	
	Wireless Power Algorithm is complete	**Wireless Power Algorithm is complete**	Informational	
Captive Portal	CP Client Connected	**CP Client Connected: MAC: <macaddr> IP: <ipaddr> SwMAC: <macaddr> CPID: <int> Interface: <int>**	Informational	
	CP Client Disconnected	**CP Client Disconnected: MAC: <macaddr> IP: <ipaddr> SwMAC: <macaddr> CPID: <int> Interface: <int>**	Informational	
	CP Client Auth Failure	**CP Client Auth Failure: MAC: <macaddr> IP: <ipaddr> SwMAC: <macaddr> CPID: <int> Interface: <int> User: <username>**	Warning	
	CP Client Authentication Database Full	**CP Client Authentication Database Full**	Informational	

Appendix D Trap Entries

This table lists the trap logs found on the Switch.

Log Entry	Description	ID
L2macNotification	This trap indicates the MAC address variations in the address table.	1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.1
L2PortSecurityViolationTrap	When the port security trap is enabled, new MAC addresses that violate the pre-defined port security configuration will trigger trap messages to be sent out.	1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.2
PortLoopOccurred	This trap is sent when a Port loop occurs.	1.3.6.1.4.1.171.12.41.10.0.1
PortLoopRestart	This trap is sent when a Port loop restarts after the interval time.	1.3.6.1.4.1.171.12.41.10.0.2
VlanLoopOccurred	This trap is sent when a Port with a VID loop occurs.	1.3.6.1.4.1.171.12.41.10.0.3
VlanLoopRestart	This trap is sent when a Port with a VID loop restarts after the interval time.	1.3.6.1.4.1.171.12.41.10.0.4
SafeGuardChgToExhausted	This trap indicates System change operation mode from normal to exhausted.	1.3.6.1.4.1.171.12.19.4.1.0.1
SafeGuardChgToNormal	This trap indicates System change operation mode from exhausted to normal.	1.3.6.1.4.1.171.12.19.4.1.0.2
MacBasedAuthLoggedSuccess	This trap is sent when a MAC-based access control host is successfully logged in.	1.3.6.1.4.1.171.12.35.11.1.0.1
MacBasedAuthLoggedFail	This trap is sent when a MAC-based access control host login fails.	1.3.6.1.4.1.171.12.35.11.1.0.2
MacBasedAuthAgesOut	This trap is sent when a MAC-based access control host ages out.	1.3.6.1.4.1.171.12.35.11.1.0.3
FilterDetectedTrap	This trap is sent when an illegal DHCP server is detected. The same illegal DHCP server IP address detected is just sent once to the trap receivers within the log ceasing unauthorized duration.	1.3.6.1.4.1.171.12.37.100.0.1
SingleIPMSColdStart	The commander Switch will send swSingleIPMSColdStart notification to the indicated	1.3.6.1.4.1.171.12.8.6.0.11
SingleIPMSWarmStart	The commander Switch will send swSingleIPMSWarmStart notification to the indicated host when its member generates a warm start notification.	1.3.6.1.4.1.171.12.8.6.0.12
SingleIPMSLinkDown	The commander Switch will send swSingleIPMSLinkDown notification to the indicated host when its member generates a link down notification.	1.3.6.1.4.1.171.12.8.6.0.13
SingleIPMSLinkUp	The commander Switch will send swSingleIPMSLinkUp notification to the indicated host when its member generates a link up notification.	1.3.6.1.4.1.171.12.8.6.0.14
SingleIPMSAuthFail	The commander Switch will send swSingleIPMSAuthFail notification to the indicated host when its member generates an authentation failure notification	1.3.6.1.4.1.171.12.8.6.0.15
SingleIPMSnewRoot	The commander Switch will send swSingleIPMSnewRoot notification to the indicated host when its member generates a new root notification.	1.3.6.1.4.1.171.12.8.6.0.16
SingleIPMSTopologyChange	The commander Switch will send swSingleIPMSTopologyChange notification to the indicated host when its member generates a topology change notification.	1.3.6.1.4.1.171.12.8.6.0.17

coldStart	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	1.3.6.1.6.3.1.1.5.1
warmStart	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.	1.3.6.1.6.3.1.1.5.2
linkDown	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.	1.3.6.1.6.3.1.1.5.3
linkUp	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.	1.3.6.1.6.3.1.1.5.4
authenticationFailure	An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1.5.5
risingAlarm	This trap is an SNMP notification that is generated when a high capacity alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.	1.3.6.1.2.1.16.29.2.0.1
fallingAlarm	This trap is an SNMP notification that is generated when a high capacity alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.	1.3.6.1.2.1.16.29.2.0.2
newRoot	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon action of the Topology Change Timer immediately subsequent to its election. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.1
topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.2
wsModeEnabled	A wsModeEnabled trap signifies that the SNMP entity, acting in an agent role, has detected that Wireless functionality on the device is enabled.	1.3.6.1.4.1.171.12.96.11.0.1
wsModeDisabled	A wsModeDisabled trap signifies that the SNMP entity, acting in an agent role, has detected that Wireless functionality on the device is disabled.	1.3.6.1.4.1.171.12.96.11.0.2
wsManagedAPDatabaseFull	A wsAPDatabaseFull trap signifies that the SNMP entity, acting in an agent role, has detected that AP Database is full.	1.3.6.1.4.1.171.12.96.11.0.3
wsManagedAPNeighborAPListFull	A wsManagedAPNeighborListFull trap signifies that the SNMP entity, acting in an agent role,	1.3.6.1.4.1.171.12.96.11.0.4

	has detected that ManagedAP neighbor AP list is full.	
wsManagedAPNeighborClientListFull	A wsManagedAPNeighborClientListFull trap signifies that the SNMP entity, acting in an agent role, has detected that ManagedAP neighbor client list is full.	1.3.6.1.4.1.171.12.96.11.0.5
wsAPFailureListFull	A wsAPFailureListFull trap signifies that the SNMP entity, acting in an agent role, has detected that AP failure list full.	1.3.6.1.4.1.171.12.96.11.0.6
wsRFScanAPListFull	A wsRFScanAPListFull trap signifies that the SNMP entity, acting in an agent role, has detected that RF scan AP list is full.	1.3.6.1.4.1.171.12.96.11.0.7
wsClientAssociationDatabaseFull	A wsClientAssociationDatabaseFull trap signifies that the SNMP entity, acting in an agent role, has detected that client association database is full.	1.3.6.1.4.1.171.12.96.11.0.8
wsPeerSwitchDiscovered	A wsPeerSwitchDiscovered trap signifies that the SNMP entity, acting in an agent role, has detected peer Switch in the network.	1.3.6.1.4.1.171.12.96.11.0.9
wsPeerSwitchFailed	A wsPeerSwitchFailed trap signifies that the SNMP entity, acting in an agent role, has detected that peer Switch connection failed.	1.3.6.1.4.1.171.12.96.11.0.10
wsPeerSwitchUnknownProtocol	A wsPeerSwitchUnknownProtocol trap signifies that the SNMP entity, acting in an agent role, has detected unknown protocol between wireless Switch and peer Switch communication.	1.3.6.1.4.1.171.12.96.11.0.11
wsManagedAPDiscovered	A wsManagedAPDiscovered trap signifies that the SNMP entity, acting in an agent role, has detected the managed AP.	1.3.6.1.4.1.171.12.96.11.0.12
wsManagedAPFailed	A wsManagedAPFailed trap signifies that the SNMP entity, acting in an agent role, has detected the failed AP.	1.3.6.1.4.1.171.12.96.11.0.13
wsManagedAPUnknownProtocol	A wsManagedAPUnknownProtocol trap signifies that the SNMP entity, acting in an agent role, has detected the unknown protocol between wireless Switch and managed AP communication.	1.3.6.1.4.1.171.12.96.11.0.14
wsAPAssociationFailure	A wsAPAssociationFailure trap signifies that the SNMP entity, acting in an agent role, has detected that AP association failed.	1.3.6.1.4.1.171.12.96.11.0.15
wsAPAuthenticationFailure	A wsAPAuthenticationFailure trap signifies that the SNMP entity, acting in an agent role, has detected that AP authentication failed.	1.3.6.1.4.1.171.12.96.11.0.16
wsRFScanRogueAPDetected	A wsRFScanRogueAPDetected trap signifies that the SNMP entity, acting in an agent role, has detected Rogue AP through RF Scan.	1.3.6.1.4.1.171.12.96.11.0.17
wsRFScanAPDetected	A wsRFScanAPDetected trap signifies that the SNMP entity, acting in an agent role, has detected AP through RF Scan.	1.3.6.1.4.1.171.12.96.11.0.18
wsRFScanNewClientDetected	A wsRFScanNewClientDetected trap signifies that the SNMP entity, acting in an agent role, has detected new client through RF Scan.	1.3.6.1.4.1.171.12.96.11.0.19
wsClientAssociationDetected	A wsClientAssociationDetected trap signifies that the SNMP entity, acting in an agent role, has detected client association.	1.3.6.1.4.1.171.12.96.11.0.20
wsClientDisassociationDetected	A wsClientDisassociationDetected trap signifies that the SNMP entity, acting in an agent role, has detected client disassociation.	1.3.6.1.4.1.171.12.96.11.0.21
wsClientRoamDetected	A wsClientRoamDetected trap signifies that the SNMP entity, acting in an agent role, has detected client roaming.	1.3.6.1.4.1.171.12.96.11.0.22
wsClientAssociationFailure	A wsClientAssociationFailure trap signifies that	1.3.6.1.4.1.171.12.96.11.0.23

	the SNMP entity, acting in an agent role, has detected client association failure.	
wsClientAuthenticationFailure	A wsAuthenticationFailure trap signifies that the SNMP entity, acting in an agent role, has detected client authentication failure.	1.3.6.1.4.1.171.12.96.11.0.24
wsAdHocClientDetected	A wsAdHocClientDetected trap signifies that the SNMP entity, acting in an agent role, has detected Ad hoc client.	1.3.6.1.4.1.171.12.96.11.0.25
wsWLANBandwidthUtilizationExceeded	A wsWLANBandwidthUtilizationExceeded trap signifies that the SNMP entity, acting in an agent role, has detected WLAN bandwidth utilization exceeding the limit.	1.3.6.1.4.1.171.12.96.11.0.26
wsAdHocClientListFull	A wsAdHocClientListFull trap signifies that the SNMP entity, acting in an agent role, has detected that Ad hoc client database is full.	1.3.6.1.4.1.171.12.96.11.0.27
wsPeerSwitchConfigurationCommandReceived	A wsPeerSwitchConfigurationCommandReceived trap signifies that the SNMP entity, acting in an agent role, has received Configuration command from the peer Switch in the network. The config mask received is also returned in the trap.	1.3.6.1.4.1.171.12.96.11.0.28
wsPeerSwitchManagedAPLimitExceeded	A wsPeerSwitchManagedAPLimitExceeded trap signifies that the SNMP entity, acting in an agent role, has detected that the Peer Switch Managed AP database limit has exceeded.	1.3.6.1.4.1.171.12.96.11.0.29
wsClusterControllerElected	A wsClusterControllerElected trap signifies that the SNMP entity, acting in an agent role, has elected itself as Cluster Controller in the peer group.	1.3.6.1.4.1.171.12.96.11.0.32
wsClusterMaxAPExceeded	A wsClusterMaxAPExceeded trap signifies that the SNMP entity, acting in an agent role, has detected that the managed APs in the network has exceeded.	1.3.6.1.4.1.171.12.96.11.0.33
wsRoguesPresent	A wsRoguesPresent trap signifies that the SNMP entity, acting in an agent role, has detected one or more Rogues present in the network.	1.3.6.1.4.1.171.12.96.11.0.34
wsDetectedClientListFull	A wsDetectedClientListFull trap signifies that the SNMP entity, acting in an agent role, has detected that Detected client database is full.	1.3.6.1.4.1.171.12.96.11.0.35
wsRogueClientsPresent	A wsRogueClientsPresent trap signifies that the SNMP entity, acting in an agent role, has detected one or more Rogue Clients present in the network.	1.3.6.1.4.1.171.12.96.11.0.36
wsChannelPlanAlgoComplete	A wsChannelAlgorithmComplete trap signifies that the SNMP entity, acting in an agent role, has detected channel algorithm complete event.	1.3.6.1.4.1.171.12.96.11.0.37
wsPowerPlanAlgoComplete	A wsPowerAlgorithmComplete trap signifies that the SNMP entity, acting in an agent role, has detected power algorithm complete event.	1.3.6.1.4.1.171.12.96.11.0.38
wsLocallyManagedAPLimitExceeded	A wsLocallyManagedAPLimitExceeded trap signifies that the SNMP entity, acting in an agent role, has detected that the WS locally managed AP limit is exceeded.	1.3.6.1.4.1.171.12.96.11.0.41
wsAPHardwareTypeFailure	A wsAPHardwareTypeFailure trap signifies that the SNMP entity, acting in an agent role, has detected that the AP Hardware Type unsupported.	1.3.6.1.4.1.171.12.96.11.0.100
cpClientAuthenticationFailure	A cpClientAuthenticationFailure trap signifies that the SNMP entity, acting in an agent role, has detected a client authentication failure.	1.3.6.1.4.1.171.12.97.4.0.1

cpClientConnect	A cpClientConnect trap signifies that the SNMP entity, acting in an agent role, has detected a client connection.	1.3.6.1.4.1.171.12.97.4.0.2
cpClientDatabaseFull	A cpClientDatabaseFull trap signifies that the SNMP entity, acting in an agent role, has detected that client authentication database is full.	1.3.6.1.4.1.171.12.97.4.0.3
cpClientDisconnect	A cpClientDisconnect trap signifies that the SNMP entity, acting in an agent role, has detected a client disconnection."	1.3.6.1.4.1.171.12.97.4.0.4

Appendix E RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the Switch is used in the following modules: 802.1X (Port-based and Host-based), MAC-based Access Control and Captive Portal Configurations.

The description that follows explains the following RADIUS Attributes Assignment types:

- Ingress/Egress Bandwidth
- 802.1p Default Priority
- VLAN
- ACL

To assign **Ingress/Egress bandwidth by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The tables below show the parameters for bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	2 (for ingress bandwidth) 3 (for egress bandwidth)	Required
Attribute-Specific Field	Used to assign the bandwidth of a port.	Unit (Kbits)	Required

If the user has configured the bandwidth attribute of the RADIUS server (for example, ingress bandwidth 1000Kbps) and the 802.1X authentication is successful, the device will assign the bandwidth (according to the RADIUS server) to the port. However, if the user does not configure the bandwidth attribute and authenticates successfully, the device will not assign any bandwidth to the port. If the bandwidth attribute is configured on the RADIUS server with a value of “0” or more, than the effective bandwidth (100Mbps on an Ethernet port or 1Gbps on a Gigabit port) of the port will be set to no_limited.

To assign **802.1p default priority by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The tables below show the parameters for 802.1p default priority.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	4	Required
Attribute-Specific Field	Used to assign the 802.1p default priority of the port.	0-7	Required

If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and the 802.1X, or Host-based authentication is successful, the device will assign the 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute is configured on the RADIUS server is a value out of range (>7), it will not be set to the device.

To assign **VLAN by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. To use VLAN assignment, RFC3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminatior).	13 (VLAN)	Required
Tunnel-Medium-Type	This attribute indicates the transport medium being used.	6 (802)	Required
Tunnel-Private-Group-ID	This attribute indicates group ID for a particular tunneled session.	A string (VID)	Required

A summary of the Tunnel-Private-Group-ID Attribute format is shown below.

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |      Type     |    Length     |      Tag      |   String...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The table below shows the definition of Tag field (different with RFC 2868):

Tag field value	String field format	Note
0x01	VLAN name (ASCII)	A tag field of greater than 0x1F is interpreted as the first octet of the following field.
0x02	VLAN ID (ASCII)	
Others (0x00, 0x03 ~ 0x1F, >0x1F)	1. When the switch receives the VLAN setting string, it will think it is the VLAN ID first. In other words, the switch will check all existed VLAN ID and check if there is one matched. 2. If the switch can find one matched, it will move to that VLAN. 3. If the switch can not find the matched VLAN ID, it will think the VLAN setting string as a “VLAN Name”. 4. Then it will check that it can find out a matched VLAN Name.	

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3) and the 802.1X, or MAC-based Access Control authentication is successful, the port will be added to VLAN 3. However, if the user does not configure the VLAN attribute and authenticates successfully, the port will be kept in its original VLAN. If the VLAN attribute configured on the RADIUS server does not exist, the port will not be assigned to the requested VLAN.

To assign **ACL by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The table below shows the parameters for an ACL. The RADIUS ACL assignment is only used in MAC-based Access Control.

The parameters of the Vendor-Specific Attribute are:

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	12 (for ACL profile) 13 (for ACL rule)	Required

Attribute-Specific Field	Used to assign the ACL profile or rule.	ACL Command
		For example:
		ACL profile: create access_profile profile_id 6 profile_name 1 ethernet vlan 0xFFF;
		ACL rule: config access_profile profile_id 6 add access_id auto_assign ethernet vlan_id 1 port all deny;
			Required

If the user has configured the ACL attribute of the RADIUS server (for example, ACL profile: **create access_profile profile_id 6 profile_name 1 ethernet**; ACL rule: **config access_profile profile_id 6 add access_id auto_assign ethernet**), and the 802.1X or MAC-based Access Control or WAC authentication is successful, the device will assign the ACL profiles and rules according to the RADIUS server. For more information about the ACL module, please refer to the 'Access Control List (ACL) Command List' chapter.

AP RADIUS Attributes:

Since an AP configuration is determined by its physical MAC address, the administrator adds a RADIUS entry for each AP with the User-Name attribute set to the MAC address. The following table indicates the attributes that are configured in the RADIUS server entry. The vendor specific attributes are added using the D-Link vendor ID (171).

Attribute	Description	Range	Usage	Default
User-Name (1)	Ethernet Address of the AP.	Valid Ethernet MAC Address.	Required	None
User-Password (2)	A fixed password used to lookup an AP	8-63 characters, default	Required	None

	entry.	"NOPASSWORD"		
Vendor-Specific (26), D-Link (171), Location (101)	A description for the AP, often based on its location.	0-32 characters	Optional	""
Vendor-Specifc (26), D-Link (171), Mode (102)	Indicates whether this AP is managed by the Switch, by an administrator, or is a rogue AP.	Managed (1), Standalone (2), Rogue (3)	Required	None
Vendor-Specifc (26), D-Link (171), Profile-ID (103)	If AP is managed by a Switch, the ID of the configuration profile for this AP.	1-16	Required if mode is WS-Managed.	None
Vendor-Specifc (26), D-Link (171), Switch-IP (104)	If there is more than one WS using this RADIUS server, indicates the IP address of the WS to managed this AP.	Valid IP Address	Optional	None
Vendor-Specifc (26), D-Link (171), Radio-1-Chan (105)	Indicates a fixed channel for the radio.	0, 1-13, 36, 40, 44, 48, 52,56, 60, 64, 104, 108, 112,116, 120, 124, 128, 132,140, 149, 153, 157, 161,165. 0 indicates automatic channel assignment.	Optional, if defined and valid will override auto channel configuration	0
Vendor-Specifc (26), D-Link (171), Radio-2-Chan (106)	Indicates a fixed channel for the radio.	0, 1-13, 36, 40, 44, 48, 52,56, 60, 64, 104, 108, 112,116, 120, 124, 128, 132,140, 149, 153, 157, 161,165. 0 indicates automatic channel assignment.	Optional, if defined and valid will override auto channel configuration.	0
Vendor-Specifc (26), D-Link (171), Radio-1-Power (107)	Indicates a fixed power setting for the radio.	0, 1-100 percent 0 indicates automatic power assignment.	Optional, if defined and valid will override auto power configuration.	0
Vendor-Specifc (26), D-Link (171), Radio-2-Power (108)	Indicates a fixed power setting for the radio.	0, 1-100 percent 0 indicates automatic power assignment.	Optional, if defined and valid wil override auto power configuration.	0
Vendor-Specifc (26), D-Link (171), Expected-Channel (112)	The expected channel for a stand-alone AP.	0, 1-165. 0 indicates that this AP can operate on any channel.	Optional	0
Vendor-Specifc (26), D-Link (171), Expected-AP-Security	The expected security mode for a stand-alone AP.	0 - Any Mode 1 - Open 2 - WEP	Optional	0

(110)		3 - WPA or WPA2		
Vendor-Specifc (26), D-Link (171), Expected-SSID (109)	The expected SSID for a standalone AP.	Character string, 0 to 32 bytes. If string is empty, then device may use any SSID	Optional	“”
Vendor-Specifc (26), D-Link (171), Allowed-On-Wired-Network (113)	Flag indicating whether this stand-alone AP is allowed on the wired network.	0 - AP is allowed on the wired network. 1 - AP is not allowed on the wired network.	Optional	0

Client 802.1X RADIUS Attributes:

An Access Point can use 802.1X authentication via the RADIUS to allow or prohibit access to the wireless network for specific users on client stations. Wireless Client QoS parameters can be obtained if (and only if) 802.1X authentication is used, which is based on user name and password identification credentials. Each of the QoS parameters defined here are optional, meaning they may not be present in the client's RADIUS server entry even though a valid 802.1X authentication occurs for the client. Assuming a wireless client successfully authenticates using 802.1X, each QoS RADIUS attribute that exists for the client will be sent to the AP for processing.

In all other cases, either 802.1X authentication is not used, is used but is not successful, or is successful but a particular QoS RADIUS attribute is either not configured or not valid for the client entry. The corresponding AP network client QoS default parameter is used instead for the client. Each such RADIUS attribute is evaluated this way, case-by-case.

Attribute	Description	Range	Usage
Vendor-Specific (26), D-Link (171), Client-ACL-Dn (120)	Access list identifier to be applied to 802.1X authenticated wireless client traffic in the outbound (down) direction. If this attribute is not present then the Client QoS Default ACL Down Type and Name parameters defined in the Network configuration are used instead. If this attribute is present but refers to an undefined access list name in the system, all packets for this client will be dropped until the ACL is defined.	Type: string 5-36 characters (not null-terminated) The string is of the form "type:name" where: • type = ACL type identifier: IPV4, IPV6, MAC • : = required separator character • name = 1-31 alphanumeric characters, specifying the ACL number (IPV4) or name (IPV6, MAC)	Optional
Vendor-Specific (26), D-Link (171), Client-ACL-Up (121)	Access list identifier to be applied to 802.1X authenticated wireless client traffic in the inbound (up) direction. If this attribute is not present then the Client QoS Default ACL Up Type and Name parameters defined in the	Type: string 5-36 characters (not null-terminated) The string is of the form	Optional

	Network configuration are used instead. If this attribute is present but refers to an undefined access list name in the system, all packets for this client will be dropped until the ACL is defined.	"type:name" where: • type = ACL type identifier: IPV4, IPV6, MAC • : = required separator character • name = 1-31 alphanumeric characters, specifying the ACL number (IPV4) or name (IPV6, MAC)	
Vendor-Specific (26), D-Link (171), Client-Policy-Dn (122)	Name of DiffServ policy to be applied to 802.1X authenticated wireless client traffic in the outbound (down) direction. If this attribute is not present then the Client QoS Default Policy Down parameter defined in the Network configuration is used instead. If this attribute is present but refers to an undefined policy name in the system, all packets for this client will be dropped until the DiffServ policy is defined.	Type: string 1-31 characters (not null-terminated)	Optional
Vendor-Specific (26), D-Link (171), Client-Policy-Up (123)	Name of DiffServ policy to be applied to 802.1X authenticated wireless client traffic in the inbound (up) direction. If this attribute is not present then the Client QoS Default Policy Up parameter defined in the Network configuration is used instead. If this attribute is present but refers to an undefined policy name in the system, all packets for this client will be dropped until the DiffServ policy is defined.	Type: string 1-31 characters (not null-terminated)	Optional
Tunnel-Type (64)	For dynamic VLAN usage.	VLAN (13)	Optional
Tunnel-Medium-Type (65)	For dynamic VLAN usage.	802	Optional
Tunnel-Private-Group-ID (81)	For dynamic VLAN usage.	VLANID	Optional

Known Client and MAC Authentication RADIUS Attributes:

The database is used to retrieve client descriptive names from the RADIUS server as well as implement MAC Authentication. An Access Point can be configured to use MAC authentication via the RADIUS to allow or deny specific client stations access to the wireless network. This is less secure but can be used for client stations that do not support 802.1X. The following table indicates the attributes that are configured in the RADIUS server entry.

Attribute	Description	Range	Usage	Default
User-Name (1)	Ethernet Address of the client station.	Valid Ethernet MAC Address.	Required	None
User-Password (2)	A fixed password used to lookup an client MAC entry.	“NOPASSWORD”	Required	None
Vendor-Specific (26), D-Link (171), MAC-Authentication-Action (114)	Flag indicating what action to take if MAC authentication is enabled on the network.	0-Global Action 1-Grant Access 2-Deny Access	Optional	0
Vendor-Specifc (26), D-Link (171), Client-Nickname (115)	Descriptive Name of the client.	0-32 Character String	Optional	“”
Tunnel-Type (64)	For dynamic VLAN usage.	VLAN (13)	Optional	
Tunnel-Medium-Type (65)	For dynamic VLAN usage.	802	Optional	
Tunnel-Private-Group-ID (81)	For dynamic VLAN usage.	VLANID	Optional	

If the global MAC Authentication action is configured as “White List”, then any wireless clients with MAC addresses that are specified in the list, and are not explicitly denied access, are granted access. If MAC address is not in the list, then the access to the client is denied.

If the global MAC Authentication action is configured as “Black List”, then any wireless clients with MAC addresses that are specified in the list, and are not explicitly granted access, are denied access. If MAC address is not in the list, then the access to the client is granted.

Captive Portal RADIUS Attributes:

The following table indicates the RADIUS attributes that are used to configure Captive Portal users. The table indicates both RADIUS attributes and vendor specific attributes (VSA) that are used to configure Captive Portal.

Attribute	Description	Range	Usage	Default
User-Name (1)	User name to be authorized	1-32 characters	Required	None
User-Password (2)	User password	8-64 characters	Required	None
Session-Timeout (27)	Logout once session timeout is reached (seconds). If the attribute is 0 or not present, then use the value configured for the Captive Portal.	Integer (seconds)	Optional	86400
Idle-Timeout (28)	Logout once idle timeout is reached (seconds). If the	Integer (seconds)	Optional	0

	attribute is 0 or not present, then use the value configured for the Captive Portal.			
Vendor-Specific (26), WISPr (14122), WISPr-Bandwidth-Max-Down (8)	Maximum client receive rate (b/s). Limits the bandwidth at which the client can receive data from the network. If the attribute is 0 or not present, then use the value configured for the Captive Portal.	Integer	Optional	0
Vendor-Specific (26), WISPr (14122), WISPr-Bandwidth-Max-Up (7)	Maximum client transmit rate (b/s). Limits the bandwidth at which the client can send data into the network. If the attribute is 0 or not present, then use the value configured for the Captive Portal.	Integer	Optional	0
Vendor-Specific (26), D-Link (171), LVL7-Max-Input-Octets (124)	Maximum number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected. If the attribute is 0 or not present, then use the value configured for the Captive Portal.	Integer	Optional	0
Vendor-Specific (26), D-Link (171), LVL7-Max-Output-Octets (125)	Maximum number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected. If the attribute is 0 or not present, then use the value configured for the Captive Portal.	Integer	Optional	0
Vendor-Specific (26), D-Link (171), LVL7-Max-Total-Octets (126)	Maximum number of octets the user is allowed to transfer (sum of octets transmitted and received). After this limit has been reached the user will be disconnected. If the attribute is 0 or not present, then use the value configured for the Captive Portal.	Integer	Optional	0

Vendor-Specific (26), D-Link (171), LVL7-Captive-Portal-Groups (127)	Acomma-delimited list of group names that correspond to the configured CP instance configurations.	String	Optional	None. The default group is used if not defined here.

Appendix F Wireless Switch Specific

Captive Portal Guidlines

Authenticated Roaming and Clustering:

In addition to the generic implementation, Captive Portal also provides two key features for the wireless networks called **authenticated roaming** and **clustering**.

1. Authenticated roaming allows the client to roam from access point to access point in a seamless fashion while remaining authenticated.
2. Clustering provides roaming between access points attached to different switches and monitoring Captive Portal status for all switches from the Cluster Controller.

The Switches in the cluster must share the same Captive Portal settings, such as Captive Portal Configuration instances, associated interfaces, local user database and RADIUS server settings. The databases should be synchronized in a cluster to support client authenticated roaming.

Cluster Controller Election

Each Switch in the peer group makes an independent decision about who is the Cluster Controller. If a Switch does not have any peer Switches, then it appoints itself the Cluster Controller.

When two Switches detect each other through the discovery process, they compare the value of the Cluster priority field. The Switch with higher priority becomes the Cluster Controller. If the priority is the same, then the Switch with lower IP address becomes the Cluster Controller. The Cluster priority is conveyed in the initial identification message

The Cluster priority has a range from 0 to 255. Setting the priority to 0, disables the Cluster Controller function on the Switch. Customers may want to disable the low-end Switches from becoming the Cluster Controller if they deploy a large network where only a high end switch or network appliance is powerful enough to act as the Cluster Controller.

The administrator may change the Switch Cluster priority value after the Switch has already joined the peer group. The Cluster priority is also conveyed in the keep-alive message enabling the peer Switches to learn the new Cluster priority of the Switch.

A Switch performs the election process after it boots, after it loses connection to the current Cluster Controller, and every time it receives an initial identification message or a keep-alive message from another Switch. The Switch keeps a list of Cluster priorities and IP addresses for each peer Switch and elects the Cluster Controller based on the criteria described above.

If a Cluster Controller Switch decides that it is no longer a controller because it receives a message from another Switch with higher Cluster priority or lower IP address, then it purges some of the databases.

The decision to transition out of the Cluster Controller state is immediate. If the Switch elects itself as the Cluster Controller immediately. If the Switch elects another Switch as the Cluster Controller, then the decision to declare that Switch as the Cluster Controller is delayed for the duration of the keep-alive timer interval. If another Cluster Controller is detected during this interval, then the delay timer is restarted. The administrator looking at the Switch status during the delay period would see that the Switch is not the Cluster Controller and the Cluster Controller address is 0.0.0.0. In this release the keep-alive timer interval is fixed at 120 seconds.

Each peer Switch independently establishes connections with other peer Switches. In a transient case, it is possible that one of the Switches, that just established a connection with another Switch, does not see all the Switches that the other Switch is seeing, so that the two Switches may select different Cluster Controllers. Although the WIDS security functions do not work correctly when peer Switches disagree about which Switch is the Cluster Controller, this condition does not affect data forwarding through the network and normal operation is restored as soon as all the Switches in the peer group discover each other.

Since the Cluster Controller function may be disabled by setting the Cluster Priority to zero, it is possible that all wireless Switches in the network are configured to disable the Cluster Controller function and the network operates without the Cluster Controller.

The Cluster priority is a global Switch configuration setting. When the global configuration is pushed from one peer Switch to another, the Cluster priority is not included in this configuration because its purpose is to differentiate the preference level for the Cluster Controller function for each Switch.

There are two Switch status parameters that reflect the results of the Cluster Controller election process. The status parameters are the **IP address** of the elected Cluster Controller and a **Boolean flag** which indicates whether this Switch is the Cluster Controller. The flag does not provide extra information since it is derived from comparing the Switch’s IP address with the Cluster address, but it offers a quick way for the administrator to know whether the local Switch is the Cluster Controller.

After the Switch decides that it is the Cluster Controller, it sends an SNMP trap.

X.509 Certification Mutual Authentication

X.509 Certification Mutual Authentication:

When the wireless system is configured to perform X.509 Mutual Certificate exchange the Switches and APs configure the TLS connection to perform mutual X.509 certificate exchange. Each device compares the certificate received from the remote end-point with the local copy of the remote device's certificate. If the certificates do not match, then the TLS connection is dropped.

The X.509 certificates are auto-generated by the Switches and the APs, so the devices don't communicate with any trusted certificate authority and the administrator is not required to pay certificate maintenance fees. Each Switch holds a copy of the X.509 certificate for all other Switches and the APs it manages. Each AP holds a copy of the X.509 certificate of the Switches to which the AP may establish a connection. The certificates are distributed when the mutual authentication feature is enabled, during AP and Switch provisioning, and triggered by an administrator command.

The X.509 mutual certificate exchange is the only mechanism for peer Switches to authenticate with each other because Switches don't support pass-phrase authentication. Note that if the wireless Switch is currently managed by a cluster controller, then any provisioning request toward this Switch will fail.

When the X.509 mutual authentication is enabled the AP and peer Switch discovery is slower than when this feature is disabled because certificates are exchanged during the TLS connection setup.

Certification Overview and Usage In the Wireless System:

The TLS connection has two sides: a client side initiates the connection and the server side accepts the connection. In a Wireless System, the APs act only as TLS clients, and Switches act as either TLS clients or TLS servers. The Switch acts as a TLS client when it establishes a connection to a peer Switch.

The TLS protocol supports client verification of server certificates and mutual certificate verification. The Wireless System configures the TLS session to use mutual certificate verification when the mutual authentication mode is enabled. When the mutual authentication mode is disabled, the Wireless System uses anonymous cipher and disables certificate exchange and verification.

In order to verify the certificate each device generates a private key and an X.509 certificate. The private key is kept on the device and is not given out to other Switches or APs. The certificate contains a matching public key. The device certificate is given out to other devices in the wireless system. Data encrypted with the public key using the device's certificate can be decrypted with the device's private key.

The certificates are encoded using PEM format, which is a Base64 encoded file. The Base64 encoding uses printable ASCII characters to represent binary data. Before the certificate files can be used for certificate validation they are loaded into the OpenSSL library.

Each wireless device has a copy of a certificate of the device with which it needs to communicate. During TLS connection establishment the Wireless devices compare the certificate received on the connection setup with all available loaded certificates for other wireless devices. If a matching certificate is found then the certificate verification succeeds. The verification function does not attempt to correlate the IP address of the device with the certificate and it does not check the certificate expiration date.

The TLS connections are configured to validate the certificates only on the initial connection setup. The connection reauthentications don't trigger new certificate validation attempts.

Certificate Generation on the Access Point:

The AP auto-generates an X.509 certificate when it boots. At boot time the AP checks whether the key file and the certificate file already exists. If the files exist then the AP uses them, otherwise the AP generates the files. The /etc/uwskey.pem file contains the 1024 bit private key. The /etc/uwscert.pem file contains the X.509 certificate.

In order to regenerate the AP certificates the administrator may issue a "factory-reset" command on the AP or delete the two files from the file system and reboot the AP.

Certificate Generation on the Switch:

The Switch auto-generates an X.509 certificate and other key files when it boots. At boot time the Switch checks whether the certificate and key files exist, and if they don't then the Switch generates the files.

The administrator can re-generate the X.509 certificates used by the Wireless component. Note that Diffie-Hellman keys are not regenerated. The wireless feature should be disabled while the keys are being regenerated. If mutual authentication is enabled then the Switch must be re-provisioned before it can join the cluster.

IP Address Assignment

The Wireless Switches are assigned IP addresses by the administrator. The routing package is included into the product and the routing is enabled by default. Besides the existing System interface, the administrator may create a routing interface optionally. The wireless software automatically selects the IP Address of the lowest interface index. The System interface is always the interface with the lowest index “1”. If the System interface is deleted then the software automatically selects the IP address of a lowest index routing interface. If no interfaces are defined then the wireless function is disabled.

Disabling the interface or changing the IP address of the interface disables the wireless function. If another interface exists then the wireless function starts using it automatically.

Once an interface is selected the wireless function continues to use that interface until the interface goes down.

Changing the IP address of the network interface automatically disables and re-enables the wireless function.

The administrator has the option to disable automatic IP address assignment for the Wireless function and enter a static IPv4 address. The IP address must be the same as an address of an active routing interface in order for the Wireless function to work. If the interface with the specified address doesn’t exist or is not active then the Wireless function is disabled and the WLAN Switch Disable Reason is set to “No Active Interface for Statically Configured IP Address”.

If the static IP address is configured when the Wireless feature is already enabled then if the configured static IP address is different from the current IP address used by the Wireless feature then the Wireless feature is automatically disabled and re-enabled with the new IP address. If the configured static IP address is already being used by the Wireless feature then the Wireless feature is not disabled and service to the wireless clients is not interrupted.

IP Tunnel versus MBA and IMPB

When Wireless Switches enables IP tunneling for wireless clients, the MAC of the wireless tunnel client has the highest priority. MBA and IMPB will not work to limit the wireless tunnel client MAC.

In addition, when a wireless tunnel client is added by Wireless Switch, the Wireless Switch will notify the MBA module to remove the client MAC if it added the MAC.

In other words, MBA and IMPB will not work when the MAC belongs to a tunnel client.

To achieve IP-in-IP tunnel forwarding, the MAC addresses of the devices under the tunnel are learned and marked as “static” FDB entries on the Wireless Switch. These “static” entries would not be removed using the “clear fdb all” command nor can they be erased by using the “delete fdb <vlan_name> <macaddr>” command. They also would not aged out from the FDB table as long as the devices are still online.