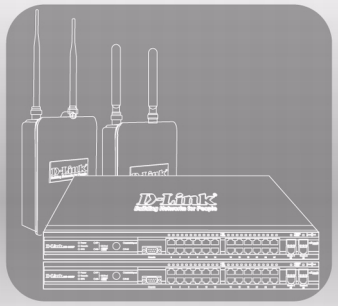
D-Link®
Building Networks for People



CLI Command Reference

Product Model: DWS-4000 Series
DWL-8600AP

Unified Wired & Wireless Access System
Release 1.0
December 2009

FCC Warning
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning
This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!
Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!
Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!
Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!
Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

VCCI Warning
この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準
に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波
妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ず
るよう要求されることがあります。

BSMI Warning
警告使用者

這是甲類的資訊產品,在居住的環境中使用時,可能會造成射頻干擾,
在這種情況下使用者會被要求採取某些適當的對策

MIC Warning
A급 기기 (업무용 정보통신기기)

이 기기는 업무용으로 전자파적합등록을 한 기기이오니
판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약
잘못판매 또는 구입하였을 때에는 가정용으로 교환하시기
바랍니다.

CCC Warning
此為 A 級產品，在生活環境中，該產品可能會造成無線電干擾，
在這種情況下，可能需要用戶對其干擾採取切實可行措施。

TABLE OF CONTENTS

LIST OF TABLES

Section 1: About This Document

This document describes command-line interface (CLI) commands you use to view and configure Unified Switch software. You can access the CLI by using a direct connection to the serial port or by using telnet or SSH over a remote network connection.

AUDIENCE

This document is for system administrators who configure and operate systems using Unified Switch software. It provides an understanding of the configuration options of the Unified Switch software.

This document assumes that the reader has an understanding of the Unified Switch software base and has read the appropriate specification for the relevant networking device platform. It also assumes that the reader has a basic knowledge of Ethernet and networking concepts.

Refer to the release notes for the Unified Switch application-level code. The release notes detail the functionality of the Switching, Routing, SNMP, Configuration, Management, and other packages.

ABOUT UNIFIED SWITCH SOFTWARE

The Unified Switch software has two purposes:

- Assist attached hardware in switching frames, based on Layer 2, 3, or 4 information contained in the frames.
- Provide a complete device management portfolio to the network administrator.

SCOPE

Unified Switch software encompasses both hardware and software support. The software is partitioned to run in the following processors:

- CPU

  This code runs the networking device management portfolio and controls the overall networking device hardware. It also assists in frame forwarding, as needed and specified. This code is designed to run on multiple platforms with minimal changes from platform to platform.

- Networking device processor

  This code does the majority of the packet switching, usually at wire speed. This code is platform dependent, and substantial changes might exist across products.

PRODUCT CONCEPT

Fast Ethernet and Gigabit Ethernet switching continues to evolve from high-end backbone applications to desktop switching applications. The price of the technology continues to decline, while performance and feature sets continue to improve.

Devices that are capable of switching Layers 2, 3, and 4 are increasingly in demand. Unified Switch software provides a flexible solution to these ever-increasing needs.

Unified Switch software includes a set of comprehensive management functions for managing both Unified Switch software and the network. You can manage the Unified Switch software by using one of the following three methods:

- Command-Line Interface (CLI)
- Simple Network Management Protocol (SNMP)
- Web-based

Each of the Unified Switch management methods enables you to configure, manage, and control the software locally or remotely using in-band or out-of-band mechanisms. Management is standards-based, with configuration parameters and a private MIB providing control for functions not completely specified in the MIBs.

Section 2: Using the Command-Line Interface

The command-line interface (CLI) is a text-based way to manage and monitor the system. You can access the CLI by using a direct serial connection or by using a remote logical connection with telnet or SSH.

This section describes the CLI syntax, conventions, and modes. It contains the following subsections:

Command Syntax

A command is one or more words that might be followed by one or more parameters. Parameters can be required or optional values.

Some commands, such as **`show network`** or **`clear vlan`**, do not require parameters. Other commands, such as **`network parms`**, require that you supply a value after the command. You must type the parameter values in a specific order, and optional parameters follow required parameters. The following example describes the **`network parms`** command syntax:

Format **`network parms`** *`<ipaddr> <netmask> [gateway]`*

- **`network parms`** is the command name.
- *`<ipaddr>`* and *`<netmask>`* are parameters and represent required values that you must enter after you type the command keywords.
- *`[gateway]`* is an optional parameter, so you are not required to enter a value in place of the parameter.

The *D-Link Unified Switch CLI Command Reference* lists each command by the command name and provides a brief description of the command. Each command reference also contains the following information:

- Format shows the command keywords and the required and optional parameters.
- Mode identifies the command mode you must be in to access the command.
- Default shows the default value, if any, of a configurable setting on the device.

The **`show`** commands also contain a description of the information that the command shows.

COMMAND CONVENTIONS

In this document, the command name is in **bold** font. Parameters are in *italic font*. You must replace the parameter name with an appropriate value, which might be a name or number. Parameters are order dependent.

The parameters for a command might include mandatory values, optional values, or keyword choices. Table 1 describes the conventions this document uses to distinguish between value types.

Table 1: Parameter Conventions

Symbol	*Example*	*Description*
<> angle brackets	`<value>`	Indicates that you must enter a value in place of the brackets and text inside them.
[] square brackets	`[value]`	Indicates an optional parameter that you can enter in place of the brackets and text inside them.
{} curly braces	`{choice1 | choice2}`	Indicates that you must select a parameter from the list of choices.
| Vertical bars	`choice1 | choice2`	Separates the mutually exclusive choices.
[{}] Braces within square brackets	`[{choice1 | choice2}]`	Indicates a choice within an optional element.

COMMON PARAMETER VALUES

Parameter values might be names (strings) or numbers.To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces. Empty strings (“”) are not valid user-defined strings. Table 2 describes common parameter values and value formatting.

Table 2: Parameter Descriptions

Parameter	*Description*

ipaddr	This parameter is a valid IP address. You can enter the IP address in the following formats:
	`a (32 bits)`
	`a.b (8.24 bits)`
	`a.b.c (8.8.16 bits)`
	`a.b.c.d (8.8.8.8)`
	In addition to these formats, the CLI accepts decimal, hexadecimal and octal formats through the following input formats (where *n* is any valid hexadecimal, octal or decimal number):
	`0xn (CLI assumes hexadecimal format.)`
	`0n (CLI assumes octal format with leading zeros.)`
	`n (CLI assumes decimal format.)`

Interface or slot/port	Valid slot and port number separated by a forward slash. For example, 0/1 represents unit number 0 and port number 1.
Logical Interface	Represents a logical slot and port number. This is applicable in the case of a port-channel (LAG). You can use the logical slot/port to configure the port-channel.
Character strings	Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.

SLOT/PORT NAMING CONVENTION

Unified Switch software references physical entities such as cards and ports by using a slot/port naming convention. The Unified Switch software also uses this convention to identify certain logical entities, such as Port-Channel interfaces.

The slot number has two uses. In the case of physical ports, it identifies the card containing the ports. In the case of logical and CPU ports it also identifies the type of interface or port.

Table 3: Type of Slots

Slot Type	*Description*
Physical slot numbers	Physical slot numbers begin with zero, and are allocated up to the maximum number of physical slots.
Logical slot numbers	Logical slots immediately follow physical slots and identify port-channel (LAG) or router interfaces.
CPU slot numbers	The CPU slots immediately follow the logical slots.

The port identifies the specific physical port or logical interface being managed on a given slot.

Table 4: Type of Ports

Port Type	*Description*
Physical Ports	The physical ports for each slot are numbered sequentially starting from zero.
Logical Interfaces	Port-channel or Link Aggregation Group (LAG) interfaces are logical interfaces that are only used for bridging functions. VLAN routing interfaces are only used for routing functions. Loopback interfaces are logical interfaces that are always up.
CPU ports	CPU ports are handled by the driver as one or more physical entities located on physical slots.

Note: In the CLI and loopback interfaces do not use the slot/port format. To specify a loopback interface, you use the loopback ID.

USING THE "NO" FORM OF A COMMAND

The `no` keyword is a specific form of an existing command and does not represent a new or distinct command. Almost every configuration command has a `no` form. In general, use the `no` form to reverse the action of a command or reset a value back to the default. For example, the `no shutdown` configuration command reverses the shutdown of an interface. Use the command without the keyword `no` to re-enable a disabled feature or to enable a feature that is disabled by default. Only the configuration commands are available in the `no` form.

UNIFIED SWITCH MODULES

The Unified Switch software suite includes the following modules:

- Switching (Layer 2)
- Routing (Layer 3)
- Quality of Service
- Management (CLI, Web UI, and SNMP)
- WLAN Switching

COMMAND MODES

The CLI groups commands into modes according to the command function. Each of the command modes supports specific Unified Switch software commands. The commands in one mode are not available until you switch to that particular mode, with the exception of the User EXEC mode commands. You can execute the User EXEC mode commands in the Privileged EXEC mode.

The command prompt changes in each command mode to help you identify the current mode. Table 5 describes the command modes and the prompts visible in that mode.

Table 5: CLI Command Modes

Command Mode	*Prompt*	*Mode Description*
User EXEC	`DWS-4026>`	Contains a limited set of commands to view basic system information.
Privileged EXEC	`(DWS-4026) #`	Allows you to issue any **EXEC** command, enter the VLAN mode, or enter the Global Configuration mode.
Global Config	`DWS-4026 (Config)#`	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Config	`DWS-4026 (Vlan)#`	Groups all the VLAN commands.
Interface Config	`DWS-4026 (Interface <slot/port>)#` `DWS-4026 (Interface Loopback <id>)#`	Manages the operation of an interface and provides access to the router interface configuration commands. Use this mode to set up a physical port for a specific logical connection operation.
Line Config	`DWS-4026 (line)#`	Contains commands to configure outbound telnet settings and console interface settings.
Policy Map Config	`DWS-4026 (Config-policy-map)#`	Contains the QoS Policy-Map configuration commands.
Policy Class Config	`DWS-4026 (Config-policy-class-map)#`	Consists of class creation, deletion, and matching commands. The class match commands specify Layer 2, Layer 3, and general match criteria.
Class Map Config	`DWS-4026 (Config-class-map)#`	Contains the QoS class map configuration commands for IPv4.
Router RIP Config	`DWS-4026 (DWS-4026 (Config-router)#`	Contains the RIP configuration commands.
MAC Access-list Config	`DWS-4026 (Config-mac-access-list)#`	Allows you to create a MAC Access-List and to enter the mode containing MAC Access-List configuration commands.
TACACS Config	`DWS-4026 (Tacacs)#`	Contains commands to configure properties for the TACACS servers.
DHCP Pool Config	`DWS-4026 (Config dhcp-pool)#`	Contains the DHCP server IP address pool configuration commands.
Wireless Config Mode	`DWS-4026 (Config-wireless)#`	Contains global WLAN switch configuration commands and provides access to other WLAN command modes.

Table 5: CLI Command Modes (Cont.)

Command Mode	Prompt	Mode Description
AP Config Mode	`DWS-4026 (Config-ap)#`	Contains commands to configure entries in the local AP database, which is used for AP validation.
AP Profile Config Mode	`DWS-4026 (Config-ap-profile)#`	Contains commands to configure the default AP profile settings as well as settings for new AP profile.
AP Profile Radio Config Mode	`DWS-4026 (Config-ap-profile-radio)#`	Contains commands to modify the radio configuration parameters for an AP profile.
AP Profile VAP Config Mode	`DWS-4026 (Config-ap-profile-vap)#`	Contains commands to configure radio 1 or radio 2 within an AP profile.
Network Config Mode	`DWS-4026 (Config-network)#`	Contains commands to configure WLAN settings for up to 64 different networks.
ARP Access-List Config Mode	`DWS-4026 (Config-arp-access-list)#`	Contains commands to add ARP ACL rules in an ARP Access List.
Captive Portal Config Mode	`DWS-4026 (Config-CP)#`	Contains commands to configure global captive portal settings.
Captive Portal Instance Mode	`DWS-4026 (Config-CP 1)#`	Contains commands to configure a captive portal instance.

Table 6 explains how to enter or exit each mode.

Table 6: CLI Mode Access and Exit

Command Mode	Access Method	Exit or Access Previous Mode
User EXEC	This is the first level of access.	To exit, enter **logout**.
Privileged EXEC	From the User EXEC mode, enter **enable**	To exit to the User EXEC mode, enter **exit** or press **Ctrl-Z.**
Global Config	From the Privileged EXEC mode, enter **configure**	To exit to the Privileged EXEC mode, enter **exit**, or press **Ctrl-Z**.
VLAN Config	From the Privileged EXEC mode, enter **vlan database**	To exit to the Privileged EXEC mode, enter **exit**, or press **Ctrl-Z**.
Interface Config	From the Global Config mode, enter **interface** *<slot/port>* or **interface loopback** *<id>* or	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Line Config	From the Global Config mode, enter **lineconfig**.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Policy-Map Config	From the Global Config mode, enter **policy-map**	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Policy-Class-Map Config	From the Policy Map mode enter **class**.	To exit to the Policy Map mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Class-Map Config	From the Global Config mode, enter **class-map** and specify the optional keyword *ipv4* to specify the Layer 3 protocol for this class. See "class-map" on page 382 for more information.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Router RIP Config	From the Global Config mode, enter **router rip**.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
MAC Access-list Config	From the Global Config mode, enter **mac access-list extended** *<name>*.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
TACACS Config	From the Global Config mode, enter **tacacs-server host** *<ip-addr>* where *<ip-addr>* is the IP address of the TACACS server on your network.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
DHCP Pool Config	From the Global Config mode, enter **ip dhcp pool** *<pool-name>*.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.

Table 6: CLI Mode Access and Exit (Cont.)

Command Mode	*Access Method*	*Exit or Access Previous Mode*
DHCPv6 Pool Config	From the Global Config mode, enter **ip dhcpv6 pool** *<pool-name>*.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Wireless Config Mode	From the Global Config mode, enter **wireless**.	To exit to Global Config mode, enter **exit**. To return to User EXEC mode, enter **Ctrl-Z**.
AP Config Mode	From the Wireless Config mode, enter **ap database** *<macaddr>* where *<macaddr>* is the MAC address of the AP to configure..	To exit to Wireless Config mode, enter **exit**. To return to the User EXEC mode, enter **Ctrl-Z**.
AP Profile Config Mode	From the Wireless Config mode, enter **ap profile** *<1-16>* where *<1-16>* is the profile ID.	To exit to Wireless Config mode, enter **exit**. To return to User EXEC mode, enter **Ctrl-Z**.
AP Profile Radio Config Mode	From the AP Profile Config mode, enter **radio** *<1-2>*.	To exit to AP Profile Config mode, enter **exit**. To return to User EXEC mode, enter **Ctrl-Z**.
AP Profile VAP Config Mode	From the AP Profile Radio Config mode, enter **vap** *<0-15>* where *<0-15>* is the VAP ID.	To exit to AP Profile Radio Configmode, enter **exit**. To return to User EXEC mode, enter **Ctrl-Z**.
Network Config Mode	From the Wireless Config mode, enter **network** *<1-64>* where *<1-64>* is the network ID.	To exit to Wireless Config mode, enter **exit**. To return to User EXEC mode, enter **Ctrl-Z**.
ARP Access-List Config Mode	From the Global Config mode, enter **arp access-list**	To exit to the Global Config mode, enter the `exit` command. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Captive Portal Config Mode	From the Global Config mode, enter **captive-portal**	To exit to the Global Config mode, enter the `exit` command. To return to the User EXEC mode, enter `Ctrl-Z`.
Captive Portal Instance Mode	From the Captive Portal Config Mode, enter **configuration** *[cp-id]* where *[cp-id]* is the captive portal instance ID.	To exit to the Captive Portal Config mode, enter `exit`. To return to the User EXEC mode, enter `Ctrl-Z`.

COMMAND COMPLETION AND ABBREVIATION

Command completion finishes spelling the command when you type enough letters of a command to uniquely identify the command keyword. Once you have entered enough letters, press the spacebar or tab key to complete the word.

Command abbreviation allows you to execute a command when you have entered there are enough letters to uniquely identify the command. You must enter all of the required keywords and parameters before you enter the command.

CLI Error Messages

If you enter a command and the system is unable to execute it, an error message appears. Table 7 describes the most common CLI error messages.

Table 7: CLI Error Messages

Message Text	*Description*
`% Invalid input detected at '^' marker.`	Indicates that you entered an incorrect or unavailable command. The carat (^) shows where the invalid text is detected. This message also appears if any of the parameters or values are not recognized.
`Command not found / Incomplete command. Use ? to list commands.`	Indicates that you did not enter the required keywords or values.
`Ambiguous command`	Indicates that you did not enter enough letters to uniquely identify the command.

CLI Line-Editing Conventions

Table 8 describes the key combinations you can use to edit commands or increase the speed of command entry. You can access this list from the CLI by entering **`help`** from the User or Privileged EXEC modes.

Table 8: CLI Editing Conventions

Key Sequence	*Description*
Delete or Backspace	Delete previous character.
Ctrl-A	Go to beginning of line.
Ctrl-E	Go to end of line.
Ctrl-F	Go forward one character.
Ctrl-B	Go backward one character.
Ctrl-D	Delete current character.
Ctrl-U, X	Delete to beginning of line.
Ctrl-K	Delete to end of line.
Ctrl-W	Delete previous word.
Ctrl-T	Transpose previous character.
Ctrl-P	Go to previous line in history buffer.
Ctrl-R	Rewrites or pastes the line.
Ctrl-N	Go to next line in history buffer.
Ctrl-Y	Prints last deleted character.
Ctrl-Q	Enables serial flow.
Ctrl-S	Disables serial flow.
Ctrl-Z	Return to root command prompt.
Tab, <SPACE>	Command-line completion.

Table 8: CLI Editing Conventions (Cont.)

Key Sequence	*Description*
Exit	Go to next lower command prompt.
?	List available commands, keywords, or parameters.

USING CLI HELP

Enter a question mark (?) at the command prompt to display the commands available in the current mode.

```
(DWS-4026) >?

enable                    Enter into user privilege mode.
help                      Display help for various special keys.
logout                    Exit this session. Any unsaved changes are lost.
ping                      Send ICMP echo packets to a specified IP address.
quit                      Exit this session. Any unsaved changes are lost.
show                      Display Switch Options and Settings.
telnet                    Telnet to a remote host.
```

Enter a question mark (?) after each word you enter to display available command keywords or parameters.

```
(DWS-4026) #network ?

javamode                  Enable/Disable.
mgmt_vlan                 Configure the Management VLAN ID of the switch.
parms                     Configure Network Parameters of the router.
protocol                  Select DHCP, BootP, or None as the network config
                          protocol.
```

If the help output shows a parameter in angle brackets, you must replace the parameter with a value.

```
(DWS-4026) #network parms ?

<ipaddr>                  Enter the IP address.
```

If there are no additional command keywords or parameters, or if additional parameters are optional, the following message appears in the output:

```
<cr>                      Press Enter to execute the command
```

You can also enter a question mark (?) after typing one or more characters of a word to list the available command or parameters that begin with the letters, as shown in the following example:

```
(DWS-4026) #show m?

mac-addr-table            mac-address-table         monitor
```


ACCESSING THE CLI

You can access the CLI by using a direct console connection or by using a telnet or SSH connection from a remote management host.

For the initial connection, you must use a direct connection to the console port. You cannot access the system remotely until the system has an IP address, subnet mask, and default gateway. You can set the network configuration information manually, or you can configure the system to accept these settings from a BOOTP or DHCP server on your network. For more information, see “Network Interface Commands” on page 473.

Section 3: Switching Commands

This section describes the switching commands available in the Unified Switch CLI.

The Switching Commands section includes the following sections:

Note: The commands in this section are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

PORT CONFIGURATION COMMANDS

This section describes the commands you use to view and configure port settings.

interface

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port).

Format	**`interface`** *`<slot/port>`*
Mode	Global Config

auto-negotiate

This command enables automatic negotiation on a port.

Default	enabled
Format	**`auto-negotiate`**
Mode	Interface Config

no auto-negotiate

This command disables automatic negotiation on a port.

Note: Automatic sensing is disabled when automatic negotiation is disabled.

Format	**`no auto-negotiate`**
Mode	Interface Config

auto-negotiate all

This command enables automatic negotiation on all ports.

Default	enabled
Format	**`auto-negotiate all`**
Mode	Global Config

no auto-negotiate all

This command disables automatic negotiation on all ports.

Format	**`no auto-negotiate all`**
Mode	Global Config

description

Use this command to create an alpha-numeric description of the port.

Format	**description** *<description>*
Mode	Interface Config

mtu

Use the **mtu** command to set the maximum transmission unit (MTU) size, in bytes, for frames that ingress or egress the interface. You can use the **mtu** command to configure jumbo frame support for physical and port-channel (LAG) interfaces. For the standard Unified Switch implementation, the MTU size is a valid integer between 1522 - 9216 for tagged packets and a valid integer between 1518 - 9216 for untagged packets.

Note: To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet (IP Header + IP payload), see "ip mtu" on page 171.

Default	1518 (untagged)
Format	**mtu** *<1518-9216>*
Mode	Interface Config

no mtu

This command sets the default MTU size (in bytes) for the interface.

Format	**no mtu**
Mode	Interface Config

shutdown

This command disables a port.

Note: You can use the **shutdown** command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Format	**shutdown**
Mode	Interface Config

no shutdown

This command enables a port.

Format	**no shutdown**
Mode	Interface Config

shutdown all

This command disables all ports.

Note: You can use the **shutdown all** command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Format	**shutdown all**
Mode	Global Config

no shutdown all

This command enables all ports.

Format	**no shutdown all**
Mode	Global Config

speed

This command sets the speed and duplex setting for the interface.

Format	**speed** *{<100 | 10> <half-duplex | full-duplex>}*
Mode	Interface Config

Acceptable Values	*Definition*
100h	100BASE-T half duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

speed all

This command sets the speed and duplex setting for all interfaces.

Format	**speed all** *{<100 | 10> <half-duplex | full-duplex>}*
Mode	Global Config

Acceptable Values	*Definition*
100h	100BASE-T half duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

show port

This command displays port information.

Format `show port {<slot/port> | all}`

Mode Privileged EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: • **Mirror** - this port is a monitoring port. For more information, see "Port Mirroring" on page 94. • **PC Mbr**- this port is a member of a port-channel (LAG). • **Probe** - this port is a probe port.
Admin Mode	The Port control administration state. The port must be enabled in order for it to be allowed into the network. - May be enabled or disabled. The factory default is enabled.
Physical Mode	The desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed is set from the auto-negotiation process. Note that the maximum capability of the port (full duplex -100M) is advertised. Otherwise, this object determines the port's duplex mode and transmission rate. The factory default is Auto.
Physical Status	The port speed and duplex mode.
Link Status	The Link is up or down.
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
LACP Mode	LACP is enabled or disabled on this port.

show port protocol

This command displays the Protocol-Based VLAN information for either the entire system, or for the indicated group.

Format `show port protocol {<groupid> | all}`

Mode Privileged EXEC

Term	*Definition*
Group Name	The group name of an entry in the Protocol-based VLAN table.
Group ID	The group identifier of the protocol group.
Protocol(s)	The type of protocol(s) for this group.
VLAN	The VLAN associated with this Protocol Group.
Interface(s)	Lists the slot/port interface(s) that are associated with this Protocol Group.

SPANNING TREE PROTOCOL COMMANDS

This section describes the commands you use to configure Spanning Tree Protocol (STP). STP helps prevent network loops, duplicate messages, and network instability.

Note: STP is disabled by default. When you enable STP on the switch, STP is still disabled on each port.

Note: If STP is disabled, the system does not forward BPDU messages.

spanning-tree

This command sets the spanning-tree operational mode to enabled.

Default	disabled
Format	`spanning-tree`
Mode	Global Config

no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format	`no spanning-tree`
Mode	Global Config

spanning-tree bpdufilter

Use this command to enable BPDU Filter on the interface.

Default	disabled
Format	`spanning-tree bpdufilter`
Mode	Interface Config

no spanning-tree bpdufilter

Use this command to disable BPDU Filter on the interface.

Default	disabled
Format	`no spanning-tree bpdufilter`
Mode	Interface Config

spanning-tree bpdufilter default

Use this command to enable BPDU Filter on all the edge port interfaces.

Default	disabled
Format	`spanning-tree bpdufilter`
Mode	Global Config

no spanning-tree bpdufilter default

Use this command to disable BPDU Filter on all the edge port interfaces.

Default	disabled
Format	`no spanning-tree bpdufilter default`
Mode	Global Config

spanning-tree bpduflood

Use this command to enable BPDU Flood on the interface.

Default	disabled
Format	`spanning-tree bpduflood`
Mode	Interface Config

no spanning-tree bpduflood

Use this command to disable BPDU Flood on the interface.

Default	disabled
Format	`no spanning-tree bpduflood`
Mode	Interface Config

spanning-tree bpduguard

Use this command to enable BPDU Guard on the switch.

Default	disabled
Format	`spanning-tree bpduguard`
Mode	Global Config

no spanning-tree bpduguard

Use this command to disable BPDU Guard on the switch.

Default	disabled
Format	`no spanning-tree bpduguard`
Mode	Global Config

spanning-tree bpdumigrationcheck

Use this command to force a transmission of rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs. Use the *<slot/port>* parameter to transmit a BPDU from a specified interface, or use the *all* keyword to transmit BPDUs from all interfaces. This command forces the BPDU transmission when you execute it, so the command does not change the system configuration or have a "no" version.

Format **spanning-tree bpdumigrationcheck** *{<slot/port> | all}*

Mode Global Config

spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The *<name>* is a string of up to 32 characters.

Default base MAC address in hexadecimal notation

Format **spanning-tree configuration name** *<name>*

Mode Global Config

no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format **no spanning-tree configuration name**

Mode Global Config

spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Default 0

Format **spanning-tree configuration revision** *<0-65535>*

Mode Global Config

no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value.

Format **no spanning-tree configuration revision**

Mode Global Config

spanning-tree edgeport

This command specifies that this port is an Edge Port within the common and internal spanning tree. This allows this port to transition to Forwarding State without delay.

Format `spanning-tree edgeport`
Mode Interface Config

no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format `no spanning-tree edgeport`
Mode Interface Config

spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value.

Default 802.1s
Format `spanning-tree forceversion` *<802.1d | 802.1s | 802.1w>*
Mode Global Config

- Use 802.1d to specify that the switch transmits ST BPDUs rather than MST BPDUs (IEEE 802.1d functionality supported).
- Use 802.1s to specify that the switch transmits MST BPDUs (IEEE 802.1s functionality supported).
- Use 802.1w to specify that the switch transmits RST BPDUs rather than MST BPDUs (IEEE 802.1w functionality supported).

no spanning-tree forceversion

This command sets the Force Protocol Version parameter to the default value.

Format `no spanning-tree forceversion`
Mode Global Config

spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to “(Bridge Max Age / 2) + 1”.

Default 15
Format `spanning-tree forward-time` *<4-30>*
Mode Global Config

no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value.

Format	**no spanning-tree forward-time**
Mode	Global Config

spanning-tree guard

This command selects whether loop guard or root guard is enabled on an interface. If neither is enabled, then the port operates in accordance with the multiple spanning tree protocol.

Default	none
Format	**spanning-tree guard** *{ none | root | loop }*
Mode	Interface Config

no spanning-tree guard

This command disables loop guard or root guard on the interface.

Format	**no spanning-tree guard**
Mode	Interface Config

spanning-tree hello-time

This command sets the Admin Hello Time parameter to a new value for the common and internal spanning tree. The hello time *<value>* is in whole seconds within a range of 1 to 10, with the value being less than or equal to *(Bridge Max Age / 2) - 1*.

Default	2
Format	**spanning-tree hello-time** *<1-10>*
Mode	Interface Config

no spanning-tree hello-time

This command sets the admin Hello Time parameter for the common and internal spanning tree to the default value.

Format	**no spanning-tree hello-time**
Mode	Interface Config

spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to *2 x (Bridge Forward Delay - 1)*.

Default	20
Format	**spanning-tree max-age** *<6-40>*
Mode	Global Config

no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value.

Format	**no spanning-tree max-age**
Mode	Global Config

spanning-tree max-hops

This command sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 1 to 127.

Default	20
Format	**spanning-tree max-hops** *<1-127>*
Mode	Global Config

no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Format	**no spanning-tree max-hops**
Mode	Global Config

spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If you specify an *<mstid>* parameter that corresponds to an existing multiple spanning tree instance, the configurations are done for that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *<mstid>*, the configurations are done for the common and internal spanning tree instance.

If you specify the **cost** option, the command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *<mstid>* parameter. You can set the path cost as a number in the range of 1 to 200000000 or **auto**. If you select **auto** the path cost value is set based on Link Speed.

If you specify the **external-cost** option, this command sets the external-path cost for MST instance 0 i.e. CIST instance. You can set the external cost as a number in the range of 1 to 200000000 or **auto**. If you specify auto, the external path cost value is set based on Link Speed.

If you specify the **port-priority** option, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *<mstid>* parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Default	• cost—auto • external-cost—auto • port-priority—128
Format	**spanning-tree mst** <*mstid> {{cost <1-200000000>	auto}	{external-cost <1-200000000>	auto}	port-priority <0-240>}*
Mode	Interface Config

no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance, or in the common and internal spanning tree to the respective default values. If you specify an *<mstid>* parameter that corresponds to an existing multiple spanning tree instance, you are configuring that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *<mstid>*, you are configuring the common and internal spanning tree instance.

If the you specify **cost**, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *<mstid>* parameter, to the default value, i.e. a path cost value based on the Link Speed.

If you specify **external-cost**, this command sets the external path cost for this port for mst 0 instance, to the default value, i.e. a path cost value based on the Link Speed.

If you specify **port-priority**, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *<mstid>* parameter, to the default value.

Format	**no spanning-tree mst** *<mstid> <cost | external-cost | port-priority>*
Mode	Interface Config

spanning-tree mst instance

This command adds a multiple spanning tree instance to the switch. The parameter *<mstid>* is a number within a range of 1 to 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by the switch is 4.

Default	none
Format	**spanning-tree mst instance** *<mstid>*
Mode	Global Config

no spanning-tree mst instance

This command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Format	**no spanning-tree mst instance** *<mstid>*
Mode	Global Config

spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 61440 in increments of 4096.

If you specify 0 (defined as the default CIST ID) as the *<mstid>*, this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value is a number within a range of 0 to 61440. The

twelve least significant bits are masked according to the 802.1s specification. This causes the priority to be rounded down to the next lower valid priority.

Default	32768
Format	**spanning-tree mst priority** *<mstid> <0-61440>*
Mode	Global Config

no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance.

If 0 (defined as the default CIST ID) is passed as the *<mstid>*, this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value.

Format	**no spanning-tree mst priority** *<mstid>*
Mode	Global Config

spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance. The vlan range can be specified as a list or as a range of values. To specify a list of VLANs, enter a list of VLAN IDs, each separated by a comma with no spaces in between. To specify a range of VLANs, separate the beginning and ending VLAN ID with a dash (-).

Format	**spanning-tree mst vlan** *<mstid> <vlanid>*
Mode	Global Config

no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are again associated with the common and internal spanning tree.

Format	**no spanning-tree mst vlan** *<mstid> <vlanid>*
Mode	Global Config

spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.

Default	disabled
Format	**spanning-tree port mode**
Mode	Interface Config

no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled.

Format `no spanning-tree port mode`

Mode Interface Config

spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

Default disabled

Format `spanning-tree port mode all`

Mode Global Config

no spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to disabled.

Format `no spanning-tree port mode all`

Mode Global Config

show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Format `show spanning-tree`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Bridge Priority	Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is displayed in multiples of 4096.
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	Time in seconds.
Topology Change Count	Number of times changed.
Topology Change	Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Value of the Root Path Cost parameter for the common and internal spanning tree.
Root Port Identifier	Identifier of the port to access the Designated Root for the CST
Root Port Max Age	Derived value.

Term	*Definition*
Root Port Bridge Forward Delay	Derived value.
Hello Time	Configured value of the parameter for the CST.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).
Bridge Max Hops	Bridge max-hops count for the device.
CST Regional Root	Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
Regional Root Path Cost	Path Cost to the CST Regional Root.
Associated FIDs	List of forwarding database identifiers currently associated with this instance.
Associated VLANs	List of VLAN IDs currently associated with this instance.

show spanning-tree brief

This command displays spanning tree settings for the bridge. The following information appears.

Format `show spanning-tree brief`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Bridge Priority	Configured value.
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Bridge Max Age	Configured value.
Bridge Max Hops	Bridge max-hops count for the device.
Bridge Hello Time	Configured value.
Bridge Forward Delay	Configured value.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *<slot/port>* is the desired switch port. The following details are displayed on execution of the command.

Format `show spanning-tree interface` *<slot/port>*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Hello Time	Admin hello time for this port.
Port Mode	Enabled or disabled.

Term	*Definition*
BPDU Guard Effect	Enabled or disabled.
Root Guard	Enabled or disabled.
Loop Guard	Enabled or disabled.
TCN Guard	Enable or disable the propagation of received topology change notifications and topology changes to other ports.
BPDU Filter Mode	Enabled or disabled.
BPDU Flood Mode	Enabled or disabled.
Auto Edge	To enable or disable the feature that causes a port that has not seen a BPDU for **edge delay** time, to become an edge port and transition to forwarding faster.
Port Up Time Since Counters Last Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent.
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.
RSTP BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.
RSTP BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance. The *<slot/port>* is the desired switch port.

Format **show spanning-tree mst port detailed** *<mstid> <slot/port>*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
MST Instance ID	The ID of the existing MST instance.
Port Identifier	The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port Priority	The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16.
Port Forwarding State	Current spanning tree state of this port.
Port Role	Each enabled MST Bridge Port receives a Port Role for each spanning tree. The port role is one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port

Term	*Definition*
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled.
Port Path Cost	Configured value of the Internal Port Path Cost parameter.
Designated Root	The Identifier of the designated root for this port.
Root Path Cost	The path cost to get to the root bridge for this instance. The root path cost is zero if the bridge is the root bridge for that instance.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

If you specify 0 (defined as the default CIST ID) as the *<mstid>*, this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *<slot/port>* is the desired switch port. In this case, the following are displayed.

Term	*Definition*
Port Identifier	The port identifier for this port within the CST.
Port Priority	The priority of the port within the CST.
Port Forwarding State	The forwarding state of the port within the CST.
Port Role	The role of the specified interface within the CST.
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled or not (disabled).
Port Path Cost	The configured path cost for the specified interface.
Auto-Calculate External Port Path Cost	Indicates whether auto calculation for external port path cost is enabled.
External Port Path Cost	The cost to get to the root bridge of the CIST across the boundary of the region. This means that if the port is a boundary port for an MSTP region, then the external path cost is used.
Designated Root	Identifier of the designated root for this port within the CST.
Root Path Cost	The root path cost to the LAN by the port.
Designated Bridge	The bridge containing the designated port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Topology Change Acknowledgement	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
Hello Time	The hello time in use for this port.
Edge Port	The configured value indicating if this port is an edge port.

Term	*Definition*
Edge Port Status	The derived value of the edge port status. True if operating as an edge port; false otherwise.
Point To Point MAC Status	Derived value indicating if this port is part of a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Internal Root Path Cost	The internal root path cost to the LAN by the designated external port.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter *<mstid>* indicates a particular MST instance. The parameter {*<slot/port>* | *all*} indicates the desired switch port or all ports.

If you specify 0 (defined as the default CIST ID) as the *<mstid>*, the status summary displays for one or all ports within the common and internal spanning tree.

Format **show spanning-tree mst port summary** *<mstid> {<slot/port> | all}*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
MST Instance ID	The MST instance associated with this port.
Interface	Valid slot and port number separated by a forward slash.
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Format `show spanning-tree mst summary`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
MST Instance ID List	List of multiple spanning trees IDs currently configured.
For each MSTID: • Associated FIDs • Associated VLANs	• List of forwarding database identifiers associated with this instance. • List of VLAN IDs associated with this instance.

show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format `show spanning-tree summary`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Spanning Tree Adminmode	Enabled or disabled.
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.
BPDU Guard Mode	Enabled or disabled.
BPDU Filter Mode	Enabled or disabled.
Configuration Name	Identifier used to identify the configuration currently being used.
Configuration Revision Level	Identifier used to identify the configuration currently being used.
Configuration Digest Key	A generated Key used in the exchange of the BPDUs.
Configuration Format Selector	Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.
MST Instances	List of all multiple spanning tree instances configured on the switch.

show spanning-tree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The *<vlanid>* corresponds to an existing VLAN ID.

Format **show spanning-tree vlan** *<vlanid>*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
VLAN Identifier	The VLANs associated with the selected MST instance.
Associated Instance	Identifier for the associated multiple spanning tree instance or “CST” if associated with the common and internal spanning tree.

VLAN COMMANDS

This section describes the commands you use to configure VLAN settings.

vlan database

This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics.

Format **vlan database**

Mode Privileged EXEC

network mgmt_vlan

This command configures the Management VLAN ID.

Default 1

Format **network mgmt_vlan** *<1-3965>*

Mode Privileged EXEC

no network mgmt_vlan

This command sets the Management VLAN ID to the default.

Format **no network mgmt_vlan**

Mode Privileged EXEC

vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 2-3965.

Format **vlan** *<2-3965>*
Mode VLAN Config

no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The VLAN range is 2-3965.

Format **no vlan** *<2-3965>*
Mode VLAN Config

vlan acceptframe

This command sets the frame acceptance mode per interface. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default all
Format **vlan acceptframe** *{vlanonly | all}*
Mode Interface Config

no vlan acceptframe

This command resets the frame acceptance mode for the interface to the default value.

Format **no vlan acceptframe**
Mode Interface Config

vlan ingressfilter

This command enables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default disabled
Format **vlan ingressfilter**
Mode Interface Config

no vlan ingressfilter

This command disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format `no vlan ingressfilter`

Mode Interface Config

vlan makestatic

This command changes a dynamically created VLAN (one that is created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-3965.

Format `vlan makestatic <2-3965>`

Mode VLAN Config

vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1-3965.

Default
- VLAN ID 1 - default
- other VLANS - blank string

Format `vlan name <1-3965> <name>`

Mode VLAN Config

no vlan name

This command sets the name of a VLAN to a blank string.

Format `no vlan name <1-3965>`

Mode VLAN Config

vlan participation

This command configures the degree of participation for a specific interface in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number.

Format `vlan participation {exclude | include | auto} <1-3965>`

Mode Interface Config

Participation options are:

Participation Options	*Definition*
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.

Participation Options	*Definition*
auto	The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

Format **vlan participation all** *{exclude | include | auto} <1-3965>*

Mode Global Config

You can use the following participation options:

Participation Options	*Definition*
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces.

Default all

Format **vlan port acceptframe all** *{vlanonly | all}*

Mode Global Config

The modes defined as follows:

Mode	*Definition*
VLAN Only mode	Untagged frames or priority frames received on this interface are discarded.
Admit All mode	Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.

With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

no vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces to Admit All. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Format **no vlan port acceptframe all**

Mode Global Config

vlan port ingressfilter all

This command enables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default	disabled
Format	**vlan port ingressfilter all**
Mode	Global Config

no vlan port ingressfilter all

This command disables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format	**no vlan port ingressfilter all**
Mode	Global Config

vlan port pvid all

This command changes the VLAN ID for all interface.

Default	1
Format	**vlan port pvid all** *<1-3965>*
Mode	Global Config

no vlan port pvid all

This command sets the VLAN ID for all interfaces to 1.

Format	**no vlan port pvid** *all*
Mode	Global Config

vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	**vlan port tagging all** *<1-3965>*
Mode	Global Config

no vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format **no vlan port tagging all**
Mode Global Config

vlan protocol group

This command adds protocol-based VLAN groups to the system. The *<groupName>* is a character string of 1 to 16 characters. When it is created, the protocol group will be assigned a unique number that will be used to identify the group in subsequent commands.

Format **vlan protocol group** *<groupname>*
Mode Global Config

vlan protocol group add protocol

This command adds the *<protocol>* to the protocol-based VLAN identified by *<groupid>*. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command fails and the protocol is not added to the group. The possible values for protocol are *ip, arp,* and *ipx*.

Default none
Format **vlan protocol group add protocol** *<groupid> <protocol>*
Mode Global Config

no vlan protocol group add protocol

This command removes the *<protocol>* from this protocol-based VLAN group that is identified by this *<groupid>*. The possible values for protocol are *ip, arp,* and *ipx*.

Format **no vlan protocol group add protocol** *<groupid> <protocol>*
Mode Global Config

vlan protocol group remove

This command removes the protocol-based VLAN group that is identified by this *<groupid>*.

Format **vlan protocol group remove** *<groupid>*
Mode Global Config

protocol group

This command attaches a *<vlanid>* to the protocol-based VLAN identified by *<groupid>*. A group may only be associated with one VLAN at a time, however the VLAN association can be changed.

Default	none
Format	**protocol group** *<groupid> <vlanid>*
Mode	VLAN Config

no protocol group

This command removes the *<vlanid>* from this protocol-based VLAN group that is identified by this *<groupid>*.

Format	**no protocol group** *<groupid> <vlanid>*
Mode	VLAN Config

protocol vlan group

This command adds the physical interface to the protocol-based VLAN identified by *<groupid>*. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface(s) are not added to the group.

Default	none
Format	**protocol vlan group** *<groupid>*
Mode	Interface Config

no protocol vlan group

This command removes the interface from this protocol-based VLAN group that is identified by this *<groupid>*.

Format	**no protocol vlan group** *<groupid>*
Mode	Interface Config

protocol vlan group all

This command adds all physical interfaces to the protocol-based VLAN identified by *<groupid>*. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

Default	none
Format	**protocol vlan group all** *<groupid>*
Mode	Global Config

no protocol vlan group all

This command removes all interfaces from this protocol-based VLAN group that is identified by this *<groupid>*.

Format	**no protocol vlan group all** *<groupid>*
Mode	Global Config

vlan pvid

This command changes the VLAN ID per interface.

Default	1
Format	**vlan pvid** *<1-3965>*
Mode	Interface Config

no vlan pvid

This command sets the VLAN ID per interface to 1.

Format	**no vlan pvid**
Mode	Interface Config

vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	**vlan tagging** *<1-3965>*
Mode	Interface Config

no vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	**no vlan tagging** *<1-3965>*
Mode	Interface Config

vlan association subnet

This command associates a VLAN to a specific IP-subnet.

Format	**vlan association subnet** *<ipaddr> <netmask> <vlanid>*
Mode	VLAN Config

no vlan association subnet

This command removes association of a specific IP-subnet to a VLAN.

Format	**no vlan association subnet** *<ipaddr> <netmask>*
Mode	VLAN Config

vlan association mac

This command associates a MAC address to a VLAN.

Format	**vlan association mac** *<macaddr> <vlanid>*
Mode	VLAN database

no vlan association mac

This command removes the association of a MAC address to a VLAN.

Format	**no vlan association mac** *<macaddr>*
Mode	VLAN database

show vlan

This command displays detailed information, including interface information, for a specific VLAN. The ID is a valid VLAN identification number.

Format	**show vlan** *<vlanid>*
Mode	• Privileged EXEC • User EXEC

Term	*Definition*
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 3965.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of “Default.” This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).
Interface	Valid slot and port number separated by a forward slash. It is possible to set the parameters for all ports by using the selectors on the top line.
Current	The degree of participation of this port in this VLAN. The permissible values are: • **Include** - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • **Exclude** - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • **Autodetect** - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Configured	The configured degree of participation of this port in this VLAN. The permissible values are: • **Include** - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • **Exclude** - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • **Autodetect** - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.

Term	*Definition*
Tagging	The tagging behavior for this port in this VLAN. • **Tagged** - Transmit traffic for this VLAN as tagged frames. • **Untagged** - Transmit traffic for this VLAN as untagged frames.

show vlan brief

This command displays a list of all configured VLANs.

Format `show vlan brief`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 3965.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of “Default.” This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

show vlan port

This command displays VLAN port information.

Format `show vlan port` *{<slot/port> | all}*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash. It is possible to set the parameters for all ports by using the selectors on the top line.
Port VLAN ID	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.
Acceptable Frame Types	The types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
Ingress Filtering	May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.
GVRP	May be enabled or disabled.
Default Priority	The 802.1p priority assigned to tagged packets arriving on the port.

show vlan association subnet

This command displays the VLAN associated with a specific configured IP-Address and net mask. If no IP address and net mask are specified, the VLAN associations of all the configured IP-subnets are displayed.

Format **show vlan association subnet** *[<ipaddr> <netmask>]*

Mode Privileged EXEC

Term	*Definition*
IP Address	The IP address assigned to each interface.
Net Mask	The subnet mask.
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN.

show vlan association mac

This command displays the VLAN associated with a specific configured MAC address. If no MAC address is specified, the VLAN associations of all the configured MAC addresses are displayed.

Format **show vlan association mac** *[<macaddr>]*

Mode Privileged EXEC

Term	*Definition*
Mac Address	A MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN.

DOUBLE VLAN COMMANDS

This section describes the commands you use to configure double VLAN (DVLAN). Double VLAN tagging is a way to pass VLAN traffic from one customer domain to another through a Metro Core in a simple and cost effective manner. The additional tag on the traffic helps differentiate between customers in the MAN while preserving the VLAN identification of the individual customers when they enter their own 802.1Q domain.

dvlan-tunnel ethertype

This command configures the ether-type for all interfaces. The ether-type may have the values of *802.1Q*, *vMAN*, or *custom*. If the ether-type has a value of *custom*, the optional value of the custom ether type must be set to a value from 0 to 65535.

Default	vman
Format	**dvlan-tunnel ethertype** *{802.1Q | vman | custom} [0-65535]*
Mode	Global Config

mode dot1q-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface.

Default	disabled
Format	**mode dot1q-tunnel**
Mode	Interface Config

no mode dot1q-tunnel

This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Format	**no mode dot1q-tunnel**
Mode	Interface Config

mode dvlan-tunnel

Use this command to enable Double VLAN Tunneling on the specified interface.

Note: When you use the **mode dvlan-tunnel** command on an interface, it becomes a service provider port. Ports that do not have double VLAN tunneling enabled are customer ports.

Default	disabled
Format	**mode dvlan-tunnel**
Mode	Interface Config

no mode dvlan-tunnel

This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Format	**no mode dvlan-tunnel**
Mode	Interface Config

show dot1q-tunnel

Use this command without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Format	**show dot1q-tunnel** *[interface {<slot/port> | all}]*
Mode	• Privileged EXEC • User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
Mode	The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
EtherType	A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 0 to 65535.

show dvlan-tunnel

Use this command without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Format	**show dvlan-tunnel** *[interface {<slot/port> | all}]*
Mode	• Privileged EXEC • User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
Mode	The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
EtherType	A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 0 to 65535.

VOICE VLAN COMMANDS

This section describes the commands you use for Voice VLAN. Voice VLAN enables switch ports to carry voice traffic with defined priority so as to enable separation of voice and data traffic coming onto the port. The benefits of using Voice VLAN is to ensure that the sound quality of an IP phone could be safeguarded from deteriorating when the data traffic on the port is high.

Also the inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network-attached clients cannot initiate a direct attack on voice components. QoS-based on IEEE 802.1P class of service (CoS) uses classification and scheduling to sent network traffic from the switch in a predictable manner. The system uses the source MAC of the traffic traveling through the port to identify the IP phone data flow.

voice vlan (Global Config)

Use this command to enable the Voice VLAN capability on the switch.

Default disabled

Format `voice vlan`

Mode Global Config

no voice vlan (Global Config)

Use this command to disable the Voice VLAN capability on the switch.

Format `no voice vlan`

Mode Global Config

voice vlan (Interface Config)

Use this command to enable the Voice VLAN capability on the interface.

Default disabled

Format **voice vlan {vlanid** *<id>* | **dot1p** *<priority>* | **none** | **untagged}**

Mode Interface Config

You can configure Voice VLAN in one of four different ways:

Parameter	*Description*
vlan-id	Configure the IP phone to forward all voice traffic through the specified VLAN. Valid VLAN ID's are from 1 to 4094 (the max supported by the platform).
dot1p	Configure the IP phone to use 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. Valid *<priority>* range is 0 to 7.
none	Allow the IP phone to use its own configuration to send untagged voice traffic.
untagged	Configure the phone to send untagged voice traffic.

no voice vlan (Interface Config)

Use this command to disable the Voice VLAN capability on the interface.

Format	`no voice vlan`
Mode	Interface Config

voice vlan data priority

Use this command to either trust or untrust the data traffic arriving on the Voice VLAN port.

Default	trust
Format	`voice vlan data priority untrust | trust`
Mode	Interface Config

show voice vlan

Format	`show voice vlan [interface { <slot/port> | all}]`
Mode	Privileged EXEC

When the `interface` parameter is not specified, only the global mode of the Voice VLAN is displayed.

Term	*Definition*
Administrative Mode	The Global Voice VLAN mode.

When the `interface` is specified:

Term	*Definition*
Voice VLAN Mode	The admin mode of the Voice VLAN on the interface.
Voice VLAN ID	The Voice VLAN ID
Voice VLAN Priority	The do1p priority for the Voice VLAN on the port.
Voice VLAN Untagged	The tagging option for the Voice VLAN traffic.
Voice VLAN CoS Override	The Override option for the voice traffic arriving on the port.
Voice VLAN Status	The operational status of Voice VLAN on the port.

PROVISIONING (IEEE 802.1P) COMMANDS

This section describes the commands you use to configure provisioning (IEEE 802.1p,) which allows you to prioritize ports.

vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the priority is 0-7. Any subsequent per port configuration will override this configuration setting.

Format `vlan port priority all <priority>`
Mode Global Config

vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the priority is 0–7.

Default 0
Format `vlan priority <priority>`
Mode Interface Config

PROTECTED PORTS COMMANDS

This section describes commands you use to configure and view protected ports on a switch. Protected ports do not forward traffic to each other, even if they are on the same VLAN. However, protected ports can forward traffic to all unprotected ports in their group. Unprotected ports can forward traffic to both protected and unprotected ports. Ports are unprotected by default.

If an interface is configured as a protected port, and you add that interface to a Port Channel or Link Aggregation Group (LAG), the protected port status becomes operationally disabled on the interface, and the interface follows the configuration of the LAG port. However, the protected port configuration for the interface remains unchanged. Once the interface is no longer a member of a LAG, the current configuration for that interface automatically becomes effective.

switchport protected (Global Config)

Use this command to create a protected port group. The *<groupid>* parameter identifies the set of protected ports. Use the *name <name>* pair to assign a name to the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.

Note: Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default unprotected
Format `switchport protected <groupid> name <name>`
Mode Global Config

no switchport protected (Global Config)

Use this command to remove a protected port group. The *groupid* parameter identifies the set of protected ports. Use the **name** keyword to remove the name from the group.

Format	**NO switchport protected** *<groupid> name*
Mode	Global Config

switchport protected (Interface Config)

Use this command to add an interface to a protected port group. The *<groupid>* parameter identifies the set of protected ports to which this interface is assigned. You can only configure an interface as protected in one group.

Note: Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	unprotected
Format	**switchport protected** *<groupid>*
Mode	Interface Config

no switchport protected (Interface Config)

Use this command to configure a port as unprotected. The *groupid* parameter identifies the set of protected ports to which this interface is assigned.

Format	**no switchport protected** *<groupid>*
Mode	Interface Config

show switchport protected

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Format	**show switchport protected** *<groupid>*
Mode	• Privileged EXEC • User EXEC

Term	*Definition*
Group ID	The number that identifies the protected port group.
Name	An optional name of the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.
List of Physical Ports	List of ports, which are configured as protected for the group identified with <groupid>. If no port is configured as protected for this group, this field is blank.

show interfaces switchport

This command displays the status of the interface (protected/unprotected) under the groupid.

Format **show interfaces switchport** *<slot/port> <groupid>*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Name	A string associated with this group as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. This field is optional.
Protected	Indicates whether the interface is protected or not. It shows TRUE or FALSE. If the group is a multiple groups then it shows TRUE in Group *<groupid>*.

GARP COMMANDS

This section describes the commands you use to configure Generic Attribute Registration Protocol (GARP) and view GARP status. The commands in this section affect both GARP VLAN Registration Protocol (GVRP) and GARP Multicast Registration Protocol (GMRP). GARP is a protocol that allows client stations to register with the switch for membership in VLANS (by using GVMP) or multicast groups (by using GVMP).

set garp timer join

This command sets the GVRP join time for one port (Interface Config mode) or all (Global Config mode) and per GARP. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or re-registering) membership for a VLAN or multicast group. This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds). The value 20 centiseconds is 0.2 seconds.

Default 20

Format **set garp timer join** *<10-100>*

Mode
- Interface Config
- Global Config

no set garp timer join

This command sets the GVRP join time (for one or all ports and per GARP) to the default and only has an effect when GVRP is enabled.

Format **no set garp timer join**

Mode
- Interface Config
- Global Config

set garp timer leave

This command sets the GVRP leave time for one port (Interface Config mode) or all ports (Global Config mode) and only has an effect when GVRP is enabled. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. The leave time is 20 to 600 (centiseconds). The value 60 centiseconds is 0.6 seconds.

Default	60
Format	**set garp timer leave** *<20-600>*
Mode	• Interface Config • Global Config

no set garp timer leave

This command sets the GVRP leave time on all ports or a single port to the default and only has an effect when GVRP is enabled.

Format	**no set garp timer leave**
Mode	• Interface Config • Global Config

set garp timer leaveall

This command sets how frequently Leave All PDUs are generated. A Leave All PDU indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds). The value 1000 centiseconds is 10 seconds. You can use this command on all ports (Global Config mode) or a single port (Interface Config mode), and it only has an effect only when GVRP is enabled.

Default	1000
Format	**set garp timer leaveall** *<200-6000>*
Mode	• Interface Config • Global Config

no set garp timer leaveall

This command sets how frequently Leave All PDUs are generated the default and only has an effect when GVRP is enabled.

Format	**no set garp timer leaveall**
Mode	• Interface Config • Global Config

show garp

This command displays GARP information.

Format	**show garp**
Mode	• Privileged EXEC • User EXEC

Term	*Definition*
GMRP Admin Mode	The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
GVRP Admin Mode	The administrative mode of GARP VLAN Registration Protocol (GVRP) for the system.

GVRP COMMANDS

This section describes the commands you use to configure and view GARP VLAN Registration Protocol (GVRP) information. GVRP-enabled switches exchange VLAN configuration information, which allows GVRP to provide dynamic VLAN creation on trunk ports and automatic VLAN pruning.

Note: If GVRP is disabled, the system does not forward GVRP messages.

set gvrp adminmode

This command enables GVRP on the system.

Default	disabled
Format	`set gvrp adminmode`
Mode	Privileged EXEC

no set gvrp adminmode

This command disables GVRP.

Format	`no set gvrp adminmode`
Mode	Privileged EXEC

set gvrp interfacemode

This command enables GVRP on a single port (Interface Config mode) or all ports (Global Config mode).

Default	disabled
Format	`set gvrp interfacemode`
Mode	• Interface Config • Global Config

no set gvrp interfacemode

This command disables GVRP on a single port (Interface Config mode) or all ports (Global Config mode). If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

Format	`no set gvrp interfacemode`
Mode	• Interface Config • Global Config

show gvrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format **show gvrp configuration** *{<slot/port> | all}*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
Join Timer	The interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is one centisecond (0.01 seconds).
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port, which is enabled or disabled (default). If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

GMRP COMMANDS

This section describes the commands you use to configure and view GARP Multicast Registration Protocol (GMRP) information. Like IGMP snooping, GMRP helps control the flooding of multicast packets.GMRP-enabled switches dynamically register and de-register group membership information with the MAC networking devices attached to the same segment. GMRP also allows group membership information to propagate across all networking devices in the bridged LAN that support Extended Filtering Services.

Note: If GMRP is disabled, the system does not forward GMRP messages.

set gmrp adminmode

This command enables GARP Multicast Registration Protocol (GMRP) on the system.

Default disabled

Format **set gmrp adminmode**

Mode Privileged EXEC

no set gmrp adminmode

This command disables GARP Multicast Registration Protocol (GMRP) on the system.

Format `no set gmrp adminmode`

Mode Privileged EXEC

set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a single interface (Interface Config mode) or all interfaces (Global Config mode). If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled on that interface. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Default disabled

Format `set gmrp interfacemode`

Mode
- Interface Config
- Global Config

no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a single interface or all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Format `no set gmrp interfacemode`

Mode
- Interface Config
- Global Config

show gmrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format `show gmrp configuration` *{<slot/port> | all}*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	The slot/port of the interface that this row in the table describes.
Join Timer	The interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).

Term	*Definition*
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

show mac-address-table gmrp

This command displays the GMRP entries in the Multicast Forwarding Database (MFDB) table.

Format `show mac-address-table gmrp`

Mode Privileged EXEC

Term	*Definition*
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address is displayed as 8 bytes.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

PORT-BASED NETWORK ACCESS CONTROL COMMANDS

This section describes the commands you use to configure port-based network access control (802.1x). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

authentication login

This command creates an authentication login list. The *<listname>* is any character string and is not case sensitive. Up to 10 authentication login lists can be configured on the switch. When a list is created, the authentication method “local” is set as the first method.

When the optional parameters “Option1”, “Option2” and/or “Option3” are used, an ordered list of methods are set in the authentication login list. If the authentication login list does not exist, a new authentication login list is first created and then the authentication methods are set in the authentication login list. The maximum number of authentication login methods is three. The possible method values are **`local, radius`** and **`reject`**.

The value of **`local`** indicates that the user’s locally stored ID and password are used for authentication. The value of **`radius`** indicates that the user’s ID and password will be authenticated using the RADIUS server. The value of **`reject`** indicates the user is never authenticated.

To authenticate a user, the first authentication method in the user's login (authentication login list) is attempted. Unified Switch software does not utilize multiple entries in the user's login. If the first entry returns a timeout, the user authentication attempt fails.

Note: The default login list included with the default configuration can not be changed.

Format **authentication login** *<listname> [<method1> [<method2> [<method3>]]]*
Mode Global Config

no authentication login

This command deletes the specified authentication login list. The attempt to delete fails if any of the following conditions are true:

- The login list name is invalid or does not match an existing authentication login list
- The specified authentication login list is assigned to any user or to the non configured user for any component
- The login list is the default login list included with the default configuration and was not created using authentication login. The default login list cannot be deleted.

Format **no authentication login** *<listname>*
Mode Global Config

clear dot1x statistics

This command resets the 802.1x statistics for the specified port or for all ports.

Format **clear dot1x statistics** *{<slot/port> | all}*
Mode Privileged EXEC

clear radius statistics

This command is used to clear all RADIUS statistics.

Format **clear radius statistics**
Mode Privileged EXEC

dot1x default-login

This command assigns the authentication login list to use for non-configured users for 802.1x port security. This setting is over-ridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Format **dot1x default-login** *<listname>*
Mode Global Config

dot1x guest-vlan

This command configures VLAN as guest vlan on a per port basis. The command specifies an active VLAN as an IEEE 802.1x guest VLAN. The range is 1 to the maximumVLAN ID supported by the platform.

Default	disabled
Format	**dot1x guest-vlan** *<vlan-id>*
Mode	Interface Config

no dot1x guest-vlan

This command disables Guest VLAN on the interface.

Default	disabled
Format	**no dot1x guest-vlan**
Mode	Interface Config

dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is auto or mac-based. If the control mode is not auto or mac-based, an error will be returned.

Format	**dot1x initialize** *<slot/port>*
Mode	Privileged EXEC

dot1x login

This command assigns the specified authentication login list to the specified user for 802.1x port security. The *<user>* parameter must be a configured user and the *<listname>* parameter must be a configured authentication login list.

Format	**dot1x login** *<user> <listname>*
Mode	Global Config

dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant. The *<count>* value must be in the range 1 - 10.

Default	2
Format	**dot1x max-req** *<count>*
Mode	Interface Config

no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format `no dot1x max-req`
Mode Interface Config

dot1x max-users

Use this command to set the maximum number of clients supported on the port when MAC-based dot1x authentication is enabled on the port. The maximum users supported per port is dependent on the product. The *<count>* value is in the range 1 - 16.

Default 16
Format **dot1x max-users** *<count>*
Mode Interface Config

no dot1x max-users

This command resets the maximum number of clients allowed per port to its default value.

Format `no dot1x max-req`
Mode Interface Config

dot1x port-control

This command sets the authentication mode to use on the specified port. Select *force-unauthorized* to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select *force-authorized* to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select *auto* to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the mac-based option is specified, then MAC-based dot1x authentication is enabled on the port.

Note: MAC-based dot1x authentication is supported on the BCM56224, BCM56514, BCM56624, and BCM56820 platforms.

Default auto
Format **dot1x port-control** *{force-unauthorized | force-authorized | auto | mac-based}*
Mode Interface Config

no dot1x port-control

This command sets the 802.1x port control mode on the specified port to the default value.

Format `no dot1x port-control`
Mode Interface Config

dot1x port-control all

This command sets the authentication mode to use on all ports. Select *force-unauthorized* to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select *force-authorized* to specify that the

authenticator PAE unconditionally sets the controlled port to authorized. Select *auto* to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the mac-based option is specified, then MAC-based dot1x authentication is enabled on the port.

Note: MAC-based dot1x authentication is supported on the BCM56224, BCM56514, BCM56624, and BCM56820 platforms.

Default	auto
Format	**dot1x port-control all** *{force-unauthorized | force-authorized | auto | mac-based}*
Mode	Global Config

no dot1x port-control all

This command sets the authentication mode on all ports to the default value.

Format	**no dot1x port-control all**
Mode	Global Config

dot1x re-authenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is **auto** or **mac-based**. If the control mode is not **auto** or **mac-based**, an error will be returned.

Note: MAC-based dot1x authentication is supported on the BCM56224, BCM56514, BCM56624, and BCM56820 platforms.

Format	**dot1x re-authenticate** *<slot/port>*
Mode	Privileged EXEC

dot1x re-authentication

This command enables re-authentication of the supplicant for the specified port.

Default	disabled
Format	**dot1x re-authentication**
Mode	Interface Config

no dot1x re-authentication

This command disables re-authentication of the supplicant for the specified port.

Format	**no dot1x re-authentication**
Mode	Interface Config

dot1x system-auth-control

Use this command to enable the dot1x authentication support on the switch. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Default	disabled
Format	`dot1x system-auth-control`
Mode	Global Config

no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Format	`no dot1x system-auth-control`
Mode	Global Config

dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported:

Tokens	*Definition*
guest-vlan-period	The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured). The guest vlan timer is only relevant when guest vlan has been configured on that specific port.
reauth-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.
quiet-period	The value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.
tx-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.
supp-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.
server-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Default
- guest-vlan-period: 90 seconds
- reauth-period: 3600 seconds
- quiet-period: 60 seconds
- tx-period: 30 seconds
- supp-timeout: 30 seconds
- server-timeout: 30 seconds

Format **dot1x timeout** *{{guest-vlan-period <seconds>} |{reauth-period <seconds>} | {quiet-period <seconds>} | {tx-period <seconds>} | {supp-timeout <seconds>} | {server-timeout <seconds>}}*

Mode Interface Config

no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

Format **no dot1x timeout** *{guest-vlan-period | reauth-period | quiet-period | tx-period | supp-timeout | server-timeout}*

Mode Interface Config

dot1x unauthenticated-vlan

Use this command to configure the unauthenticated VLAN associated with that port. The unauthenticated VLAN ID can be a valid VLAN ID from 0-Maximum supported VLAN ID (3965 for Unified Switch Enterprise). The unauthenticated VLAN must be statically configured in the VLAN database to be operational. By default, the unauthenticated VLAN is 0, i.e. invalid and not operational.

Default 0

Format **dot1x unauthenticated-vlan** *<vlan id>*

Mode Interface Config

no dot1x unauthenticated-vlan

This command resets the unauthenticated-vlan associated with the port to its default value.

Format **no dot1x unauthenticated-vlan**

Mode Interface Config

dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The *<user>* parameter must be a configured user.

Format **dot1x user** *<user> {<slot/port> | all}*

Mode Global Config

no dot1x user

This command removes the user from the list of users with access to the specified port or all ports.

Format	**no dot1x user** *<user> {<slot/port> | all}*
Mode	Global Config

users defaultlogin

This command assigns the authentication login list to use for non-configured users when attempting to log in to the system. This setting is overridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Format	**users defaultlogin** *<listname>*
Mode	Global Config

users login

This command assigns the specified authentication login list to the specified user for system login. The *<user>* must be a configured *<user>* and the *<listname>* must be a configured login list.

If the user is assigned a login list that requires remote authentication, all access to the interface from all CLI, web, and telnet sessions will be blocked until the authentication is complete.

Note that the login list associated with the admin user can not be changed to prevent accidental lockout from the switch.

Format	**users login** *<user> <listname>*
Mode	Global Config

show authentication

This command displays the ordered authentication methods for all authentication login lists.

Format	**show authentication**
Mode	Privileged EXEC

Term	*Definition*
Authentication Login List	The authentication login listname.
Method 1	The first method in the specified authentication login list, if any.
Method 2	The second method in the specified authentication login list, if any.
Method 3	The third method in the specified authentication login list, if any.

show authentication users

This command displays information about the users assigned to the specified authentication login list. If the login is assigned to non-configured users, the user “default” will appear in the user column.

Format	**show authentication users** *<listname>*
Mode	Privileged EXEC

Term	*Definition*
User	The user assigned to the specified authentication login list.
Component	The component (User or 802.1x) for which the authentication login list is assigned.

show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the tokens used.

Format	**show dot1x** *[{summary {<slot/port> | all} | detail <slot/port> | statistics <slot/port>]*
Mode	Privileged EXEC

If you do not use the optional parameters *<slot/port>* or *<vlanid>*, the command displays the global dot1x mode and the VLAN Assignment mode.

Term	*Definition*
Administrative Mode	Indicates whether authentication control on the switch is enabled or disabled.
VLAN Assignment Mode	Indicates whether assignment of an authorized port to a RADIUS assigned VLAN is allowed (enabled) or not (disabled).

If you use the optional parameter *summary {<slot/port> | all}*, the dot1x configuration for the specified port or all ports are displayed.

Note: MAC-based dot1x authentication is supported on the BCM56224, BCM56514, BCM56624, and BCM56820 platforms.

Term	*Definition*
Interface	The interface whose configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto | mac-based | authorized | unauthorized.
Operating Control Mode	The control mode under which this port is operating. Possible values are authorized | unauthorized.
Reauthentication Enabled	Indicates whether re-authentication is enabled on this port.
Port Status	Indicates whether the port is authorized or unauthorized. Possible values are authorized | unauthorized.

If you use the optional parameter '**detail** *<slot/port>*', the detailed dot1x configuration for the specified port is displayed.

Note: MAC-based dot1x authentication is supported on the BCM56224, BCM56514, BCM56624, and BCM56820 platforms.

Term	*Definition*
Port	The interface whose configuration is displayed.
Protocol Version	The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.
PAE Capabilities	The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto | mac-based.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Quiet Period	The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Guest-VLAN ID	The guest VLAN identifier configured on the interface.
Guest VLAN Period	The time in seconds for which the authenticator waits before authorizing and placing the port in the Guest VLAN, if no EAPOL packets are detected on that port.
Supplicant Timeout	The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Server Timeout	The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.
Maximum Requests	The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.
Vlan-assigned	The VLAN assigned to the port by the radius server. This is only valid when the port control mode is not Mac-based.
VLAN Assigned Reason	The reason the VLAN identified in the VLAN-assigned field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Guest VLAN, default, and Not Assigned. When the VLAN Assigned Reason is Not Assigned, it means that the port has not been assigned to any VLAN by dot1x. This only valid when the port control mode is not MAC-based.
Reauthentication Period	The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.
Reauthentication Enabled	Indicates if reauthentication is enabled on this port. Possible values are ‘True” or “False”.
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
Control Direction	The control direction for the specified port or ports. Possible values are both or in.
Maximum Users	The maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This value is used only when the port control mode is not MAC-based.

Term	*Definition*
Unauthenticated VLAN ID	Indicates the unauthenticated VLAN configured for this port. This value is valid for the port only when the port control mode is not MAC-based.
Session Timeout	Indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default, Radius-Request. If the value is Default, the session is terminated the port goes into unauthorized state. If the value is Radius-Request, then a reauthentication of the client authenticated on the port is performed. This value is valid for the port only when the port control mode is not MAC-based.

Note: MAC-based dot1x authentication is supported on the BCM56224, BCM56514, BCM56624, and BCM56820 platforms.

For each client authenticated on the port, the `show dot1x detail <slot/port>` command will display the following MAC-based dot1x parameters if the port-control mode for that specific port is MAC-based.

Term	*Definition*
Supplicant MAC-Address	The MAC-address of the supplicant.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
VLAN-Assigned	The VLAN assigned to the client by the radius server.
Logical Port	The logical port number associated with the client.

If you use the optional parameter **`statistics`** *<slot/port>*, the following dot1x statistics for the specified port appear.

Term	*Definition*
Port	The interface whose statistics are displayed.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator.
EAPOL Start Frames Received	The number of EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPOL logoff frames that have been received by this authenticator.
Last EAPOL Frame Version	The protocol version number carried in the most recently received EAPOL frame.
Last EAPOL Frame Source	The source MAC address carried in the most recently received EAPOL frame.
EAP Response/Id Frames Received	The number of EAP response/identity frames that have been received by this authenticator.

Term	*Definition*
EAP Response Frames Received	The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
EAP Request/Id Frames Transmitted	The number of EAP request/identity frames that have been transmitted by this authenticator.
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
Invalid EAPOL Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Length Error Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

show dot1x clients

This command displays 802.1x client information.

Format **show dot1x clients** {*<slot/port> | all}*

Mode Privileged EXEC

Term	*Definition*
Logical Interface	The logical port number associated with a client.
Interface	The physical port to which the supplicant is associated.
User Name	The user name used by the client to authenticate to the server.
Supplicant MAC Address	The supplicant device MAC address.
Session Time	The time since the supplicant is logged on.
Filter ID	Identifies the Filter ID returned by the RADIUS server when the client was authenticated. This is a configured DiffServ policy name on the switch.
VLAN ID	The VLAN assigned to the port.
VLAN Assigned	The reason the VLAN identified in the VLAN ID field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, or Default. When the VLAN Assigned reason is Default, it means that the VLAN was assigned to the port because the PVID of the port was that VLAN ID.
Session Timeout	This value indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port-control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default and Radius-Request. If the value is Default, the session is terminated and client details are cleared. If the value is Radius-Request, then a reauthentication of the client is performed.

show dot1x users

This command displays 802.1x port security user information for locally configured users.

Format **show dot1x users** *<slot/port>*

Mode Privileged EXEC

Term	*Definition*
Users	Users configured locally to have access to the specified port.

show users authentication

This command displays all user and all authentication login information. It also displays the authentication login list assigned to the default user.

Format	`show users authentication`
Mode	Privileged EXEC

Term	*Definition*
User	Lists every user that has an authentication login list assigned.
System Login	The authentication login list assigned to the user for system login.
802.1x Port Security	The authentication login list assigned to the user for 802.1x port security.

802.1X SUPPLICANT COMMANDS

Unified Switch SMB supports 802.1x ("dot1x") supplicant functionality on point-to-point ports. The administrator can configure the user name and password used in authentication and capabilities of the supplicant port.

dot1x pae

This command sets the port's dot1x role. The port can serve as either a supplicant or an authenticator.

Format	**dot1x pae** *{supplicant | authenticator}*
Mode	Interface Config

dot1x supplicant port-control

This command sets the ports authorization state (Authorized or Unauthorized) either manually or by setting the port to auto-authorize upon startup. By default all the ports are authenticators. If the port's attribute needs to be moved from <authenticator to supplicant> or <supplicant to authenticator>, use this command.

Format	**dot1x supplicant port-control** *{auto | force-authorized | force_unauthorized}*
Mode	Interface Config

Parameter	*Description*
auto	The port is in the Unauthorized state until it presents its user name and password credentials to an authenticator. If the authenticator authorizes the port, then it is placed in the Authorized state.
force-authorized	Sets the authorization state of the port to Authorized, bypassing the authentication process.
force-unauthorized	Sets the authorization state of the port to Unauthorized, bypassing the authentication process.

no dot1x supplicant port-control

This command sets the port-control mode to the default, auto.

Default	auto
Format	**no dot1x supplicant port-control**
Mode	Interface Config

dot1x supplicant max-start

This command configures the number of attempts that the supplicant makes to find the authenticator before the supplicant assumes that there is no authenticator.

Default	3
Format	**dot1x supplicant max-start** *<1-10>*
Mode	Interface Config

no dot1x supplicant max-start

This command sets the max-start value to the default.

Format	**no dot1x supplicant max-start**
Mode	Interface Config

dot1x supplicant timeout start-period

This command configures the start period timer interval to wait for the EAP identity request from the authenticator.

Default	30 seconds
Format	**dot1x supplicant timeout start-period** *<1-65535 seconds>*
Mode	Interface Config

no dot1x supplicant timeout start-period

This command sets the start-period value to the default.

Format	**no dot1x supplicant timeout start-period**
Mode	Interface Config

dot1x supplicant timeout held-period

This command configures the held period timer interval to wait for the next authentication on previous authentication fail.

Default	30 seconds
Format	**dot1x supplicant timeout held-period** *<1-65535 seconds>*
Mode	Interface Config

no dot1x supplicant timeout held-period

This command sets the held-period value to the default value.

Format	**no dot1x supplicant timeout held-period**
Mode	Interface Config

dot1x supplicant timeout auth-period

This command configures the authentication period timer interval to wait for the next EAP request challenge from the authenticator.

Default	30 seconds
Format	**dot1x supplicant timeout auth-period** *<1-65535 seconds>*
Mode	Interface Config

no dot1x supplicant timeout auth-period

This command sets the auth-period value to the default value.

Format	**no dot1x supplicant timeout auth-period**
Mode	Interface Config

dot1x supplicant user

Use this command to map the given user to the port.

Format	**dot1x supplicant user**
Mode	Interface Config

show dot1x users

This command displays the dot1x supplicant user information for the specified interface.

Format	**show dot1x users** *<slot/port>*
Mode	• Privileged EXEC • User EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show dot1x users 0/6
user name
admin
guest
```

show dot1x summary

This command displays the dot1x port status.

Format `Show dot1x summary {all|<slot/port>}`

Mode
- Privileged EXEC
- User EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show dot1x summary 0/1
                                Operating
Interface  Control Mode     Control Mode     Port Status
---------  ------------     ------------     ------------
0/1        auto             auto             Authorized
```

See "show dot1x" on page 62 for a description of these fields.

show dot1x detail

This command displays the dot1x port status in detail.

Format `show dot1x detail <slot/port>`

Mode
- Privileged EXEC
- User EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show dot1x detail 0/1
Port..................................... 0/1
Protocol Version......................... 1
PAE Capabilities......................... Supplicant
Control Mode............................. auto
Supplicant PAE State..................... Initialize
Supplicant Backend Authentication State..... Initialize
Maximum Start trails..................... 3
Start Period (secs)...................... 30
Held Period (secs)....................... 60
Authentication Period (secs)............. 30
EAP Method............................... MD5-Challenge
```

See "show dot1x" on page 62 for a description of these fields.

show dot1x statistics

This command displays the dot1x port statistics in detail.

Format `show dot1x statistics <slot/port>`

Mode
- Privileged EXEC
- User EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show dot1x statistics 0/1
Port..................................... 0/1
EAPOL Frames Received.................... 0
EAPOL Frames Transmitted................. 0
```

```
EAPOL Start Frames Transmitted.................. 3
EAPOL Logoff Frames Received.................... 0
EAP Resp/Id frames transmitted.................. 0
EAP Response frames transmitted................. 0
EAP Req/Id frames transmitted................... 0
EAP Req frames transmitted...................... 0
Invalid EAPOL frames received................... 0
EAP length error frames received................ 0
Last EAPOL Frame Version........................ 0
Last EAPOL Frame Source........................ 00:00:00:00:02:01
```

STORM-CONTROL COMMANDS

This section describes commands you use to configure storm-control and view storm-control configuration information. A traffic storm is a condition that occurs when incoming packets flood the LAN, which creates performance degradation in the network. The Storm-Control feature protects against this condition.

Unified Switch provides broadcast, multicast, and unicast story recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast, multicast, and unicast storm-control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast, multicast, or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis.

Configuring a storm-control level also enables that form of storm-control. Disabling a storm-control level (using the “no” version of the command) sets the storm-control level back to the default value and disables that form of storm-control. Using the “no” version of the “storm-control” command (not stating a “level”) disables that form of storm-control but maintains the configured “level” (to be active the next time that form of storm-control is enabled.)

Note: The actual rate of ingress traffic required to activate storm-control is based on the size of incoming packets and the hard-coded average packet size of 512 bytes - used to calculate a packet-per-second (pps) rate - as the forwarding-plane requires pps versus an absolute rate kbps. For example, if the configured limit is 10%, this is converted to ~25000 pps, and this pps limit is set in forwarding plane (hardware). You get the approximate desired output when 512bytes packets are used.

storm-control broadcast

Use this command to enable broadcast storm recovery mode for a specific interface. If the mode is enabled, broadcast storm recovery is active and, if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default	disabled
Format	`storm-control broadcast`
Mode	Global Config Interface Config

no storm-control broadcast

Use this command to disable broadcast storm recovery mode for a specific interface.

Format	**`no storm-control broadcast`**
Mode	Global Config Interface Config

storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for an interface as a percentage of link speed and enable broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default	5
Format	**`storm-control broadcast level`** *`<0-100>`*
Mode	Interface Config

no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for an interface and disables broadcast storm recovery.

Format	**`no storm-control broadcast level`**
Mode	Interface Config

storm-control broadcast rate

Use this command to configure the broadcast storm recovery threshold for an interface in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default	0
Format	**`storm-control broadcast rate`** *`<0-33554431>`*
Mode	Interface Config

no storm-control broadcast rate

This command sets the broadcast storm recovery threshold to the default value for an interface and disables broadcast storm recovery.

Format	**`no storm-control broadcast rate`**
Mode	Interface Config

storm-control broadcast all

This command enables broadcast storm recovery mode for all interfaces. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default	disabled
Format	**storm-control broadcast all**
Mode	Global Config

no storm-control broadcast all

This command disables broadcast storm recovery mode for all interfaces.

Format	**no storm-control broadcast all**
Mode	Global Config

storm-control broadcast all level

This command configures the broadcast storm recovery threshold for all interfaces as a percentage of link speed and enables broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.This command also enables broadcast storm recovery mode for all interfaces.

Default	5
Format	**storm-control broadcast all level** *<0-100>*
Mode	Global Config

no storm-control broadcast all level

This command sets the broadcast storm recovery threshold to the default value for all interfaces and disables broadcast storm recovery.

Format	**no storm-control broadcast all level**
Mode	Global Config

storm-control broadcast all rate

Use this command to configure the broadcast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default	0
Format	**storm-control broadcast rate** *<0-33554431>*
Mode	Global Config

no storm-control broadcast all rate

This command sets the broadcast storm recovery threshold to the default value for all interfaces and disables broadcast storm recovery.

Format	**`no storm-control broadcast all rate`**
Mode	Global Config

storm-control multicast

This command enables multicast storm recovery mode for an interface. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	disabled
Format	**`storm-control multicast`**
Mode	Interface Config

no storm-control multicast

This command disables multicast storm recovery mode for an interface.

Format	**`no storm-control multicast`**
Mode	Interface Config

storm-control multicast level

This command configures the multicast storm recovery threshold for an interface as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	5
Format	**`storm-control multicast level`** *`<0-100>`*
Mode	Interface Config

no storm-control multicast level

This command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Format	**`no storm-control multicast level`** *`<0-100>`*
Mode	Interface Config

storm-control multicast rate

Use this command to configure the multicast storm recovery threshold for an interface in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default	0
Format	**storm-control multicast rate** *<0-33554431>*
Mode	Interface Config

no storm-control multicast rate

This command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Format	**no storm-control multicast rate**
Mode	Interface Config

storm-control multicast all

This command enables multicast storm recovery mode for all interfaces. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	disabled
Format	**storm-control multicast all**
Mode	Global Config

no storm-control multicast all

This command disables multicast storm recovery mode for all interfaces.

Format	**no storm-control multicast all**
Mode	Global Config

storm-control multicast all level

This command configures the multicast storm recovery threshold for all interfaces as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	5
Format	**storm-control multicast all level** *<0-100>*
Mode	Global Config

no storm-control multicast all level

This command sets the multicast storm recovery threshold to the default value for all interfaces and disables multicast storm recovery.

Format	**`no storm-control multicast all level`**
Mode	Global Config

storm-control multicast all rate

Use this command to configure the multicast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default	0
Format	**`storm-control multicast rate`** *`<0-33554431>`*
Mode	Global Config

no storm-control broadcast all rate

This command sets the broadcast storm recovery threshold to the default value for all interfaces and disables broadcast storm recovery.

Format	**`no storm-control broadcast all rate`**
Mode	Global Config

storm-control unicast

This command enables unicast storm recovery mode for an interface. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default	disabled
Format	**`storm-control unicast`**
Mode	Interface Config

no storm-control unicast

This command disables unicast storm recovery mode for an interface.

Format	**`no storm-control unicast`**
Mode	Interface Config

storm-control unicast level

This command configures the unicast storm recovery threshold for an interface as a percentage of link speed, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.This command also enables unicast storm recovery mode for an interface.

Default	5
Format	**storm-control unicast level** *<0-100>*
Mode	Interface Config

no storm-control unicast level

This command sets the unicast storm recovery threshold to the default value for an interface and disables unicast storm recovery.

Format	**no storm-control unicast level**
Mode	Interface Config

storm-control unicast rate

Use this command to configure the unicast storm recovery threshold for an interface in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default	0
Format	**storm-control unicast rate** *<0-33554431>*
Mode	Interface Config

no storm-control unicast rate

This command sets the unicast storm recovery threshold to the default value for an interface and disables unicast storm recovery.

Format	**no storm-control unicast rate**
Mode	Interface Config

storm-control unicast all

This command enables unicast storm recovery mode for all interfaces. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default disabled
Format `storm-control unicast all`
Mode Global Config

no storm-control unicast all

This command disables unicast storm recovery mode for all interfaces.

Format `no storm-control unicast all`
Mode Global Config

storm-control unicast all level

This command configures the unicast storm recovery threshold for all interfaces as a percentage of link speed, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default 5
Format `storm-control unicast all level` *<0-100>*
Mode Global Config

no storm-control unicast all level

This command sets the unicast storm recovery threshold to the default value and disables unicast storm recovery for all interfaces.

Format `no storm-control unicast all level`
Mode Global Config

storm-control unicast all rate

Use this command to configure the unicast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default 0
Format `storm-control unicast all rate` *<0-33554431>*
Mode Global Config

no storm-control unicast all rate

This command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Format `no storm-control unicast all rate`
Mode Global Config

storm-control flowcontrol

This command enables 802.3x flow control for the switch and only applies to full-duplex mode ports.

Note: 802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss.

Default	disabled
Format	`storm-control flowcontrol`
Mode	Global Config

no storm-control flowcontrol

This command disables 802.3x flow control for the switch.

Note: This command only applies to full-duplex mode ports.

Format	`no storm-control flowcontrol`
Mode	Global Config

show storm-control

This command displays switch configuration information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters:

- **Broadcast Storm Recovery Mode** may be enabled or disabled. The factory default is disabled.
- **802.3x Flow Control Mode** may be enabled or disabled. The factory default is disabled.

Use the **all** keyword to display the per-port configuration parameters for all interfaces, or specify the *slot/port* to display information about a specific interface.

Format	**show storm-control** *[all | <slot/port>]*
Mode	Privileged EXEC

Term	*Definition*
Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled. The factory default is disabled.
Bcast Level	The broadcast storm control level.
Mcast Mode	Shows whether the multicast storm control mode is enabled or disabled.
Mcast Level	The multicast storm control level.
Ucast Mode	Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.
Ucast Level	The Unknown Unicast or DLF (Destination Lookup Failure) storm control level.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show storm-control
802.3x Flow Control Mode..................... Disable
```

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show storm-control 0/1

        Bcast    Bcast    Mcast    Mcast    Ucast    Ucast
 Intf    Mode     Level    Mode     Level    Mode     Level
------ ------- -------- ------- -------- ------- --------
0/1     Disable       5% Disable       5% Disable       5%
```

Example: The following shows an example of part of the CLI display output for the command.

```
(DWS-4026) #show storm-control all

        Bcast    Bcast    Mcast    Mcast    Ucast    Ucast
 Intf    Mode     Level    Mode     Level    Mode     Level
------ ------- -------- ------- -------- ------- --------
0/1     Disable       5% Disable       5% Disable       5%
0/2     Disable       5% Disable       5% Disable       5%
0/3     Disable       5% Disable       5% Disable       5%
0/4     Disable       5% Disable       5% Disable       5%
0/5     Disable       5% Disable       5% Disable       5%
```

PORT-CHANNEL/LAG (802.3AD) COMMANDS

This section describes the commands you use to configure port-channels, which is defined in the 802.3AD specification, and that are also known as link aggregation groups (LAGs). Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address.Assign the port-channel (LAG) VLAN membership after you create a port-channel. If you do not assign VLAN membership, the port-channel might become a member of the management VLAN which can result in learning and switching issues.

A port-channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols.) A static port-channel interface does not require a partner system to be able to aggregate its member ports.

Note: If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

port-channel

This command configures a new port-channel (LAG) and generates a logical slot/port number for the port-channel. The *<name>* field is a character string which allows the dash "-" character as well as alphanumeric characters. Use the **`show port channel`** command to display the slot/port number for the logical interface.

Note: Before you include a port in a port-channel, set the port physical mode. For more information, see "speed" on page 16.

Format	**port-channel** *<name>*
Mode	Global Config

no port-channel

This command deletes a port-channel (LAG).

Format	**no port-channel** *{<logical slot/port> | all}*
Mode	Global Config

addport

This command adds one port to the port-channel (LAG). The first interface is a logical slot/port number of a configured port-channel.

Note: Before adding a port to a port-channel, set the physical mode of the port. For more information, see "speed" on page 16.

Format	**addport** *<logical slot/port>*
Mode	Interface Config

deleteport (Interface Config)

This command deletes the port from the port-channel (LAG). The interface is a logical slot/port number of a configured port-channel.

Format	**deleteport** *<logical slot/port>*
Mode	Interface Config

deleteport (Global Config)

This command deletes all configured ports from the port-channel (LAG). The interface is a logical slot/port number of a configured port-channel. To clear the port channels, see "clear port-channel" on page 432.

Format	**deleteport** *{<logical slot/port> | all}*
Mode	Global Config

lacp admin key

Use this command to configure the administrative value of the key for the port-channel. The value range of <*key*> is 0 to 65535.

Default	0x8000
Format	**lacp admin key** <*key*>
Mode	Interface Config

Note: This command is only applicable to port-channel interfaces.

no lacp admin key

Use this command to configure the default administrative value of the key for the port-channel.

Format `no lacp admin key`
Mode Interface Config

lacp collector max-delay

Use this command to configure the port-channel collector max delay. The valid range of <*delay*> is 0-65535.

Default 0x8000
Format `lacp collector max delay <delay>`
Mode Interface Config

Note: This command is only applicable to port-channel interfaces.

no lacp collector max delay

Use this command to configure the default port-channel collector max delay.

Format `no lacp collector max delay`
Mode Interface Config

lacp actor admin

Use this command to configure the LACP actor admin parameters.

lacp actor admin key

Use this command to configure the administrative value of the LACP actor admin key. The valid range for <*key*> is 0-65535.

Default Internal Interface Number of this Physical Port
Format `lacp actor admin key <key>`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor admin key

Use this command to configure the default administrative value of the key.

Format	`no lacp actor admin key`
Mode	Interface Config

lacp actor admin state

Use this command to configure the administrative value of actor state as transmitted by the Actor in LACPDUs. The valid value range is 0x00-0xFF.

Default	0x07
Format	`lacp actor admin state {individual|longtimeout|passive}`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor admin state

Use this command the configure the default administrative values of actor state as transmitted by the Actor in LACPDUs.

Format	`no lacp actor admin state {individual|longtimeout|passive}`
Mode	Interface Config

lacp actor admin state individual

Use this command to set LACP actor admin state to individual.

Format	`lacp actor admin state individual`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor admin state individual

Use this command to set the LACP actor admin state to aggregation.

Format	`no lacp actor admin state individual`
Mode	Interface Config

lacp actor admin state longtimeout

Use this command to set LACP actor admin state to longtimeout.

Format	`lacp actor admin state longtimeout`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor admin state longtimeout

Use this command to set the LACP actor admin state to short timeout.

Format	`no lacp actor admin state longtimeout`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

lacp actor admin state passive

Use this command to set the LACP actor admin state to passive.

Format	`lacp actor admin state passive`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor admin state passive

Use this command to set the LACP actor admin state to active.

Format	`no lacp actor admin state passive`
Mode	Interface Config

lacp actor port

Use this command to configure LACP actor port priority key.

lacp actor port priority

Use this command to configure the priority value assigned to the Aggregation Port. The valid range for <*priority*> is 0 to 255.

Default	0x80
Format	`lacp actor port priority` <*priority*>
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor port priority

Use this command to configure the default priority value assigned to the Aggregation Port.

Format	**no lacp actor port priority**
Mode	Interface Config

lacp actor system priority

Use this command to configure the priority value associated with the LACP Actor's SystemID. The range for <*priority*> is 0 to 255.

Default	0x80
Format	**lacp actor system priority** <*priority*>
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor system priority

Use this command to configure the priority value associated with the Actor's SystemID.

Format	**lacp actor system priority**
Mode	Interface Config

lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner. The valid range for <*key*> is 0 to 65535.

Default	0x0
Format	**lacp partner admin key** <*key*>
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner.

Format	**no lacp partner admin key** <*key*>
Mode	Interface Config

lacp partner admin state

Use this command to configure the current administrative value of actor state for the protocol Partner. The valid value range is 0x00-0xFF.

Default	0x07
Format	**lacp partner admin state** *{individual|longtimeout|passive}*
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner admin state

Use this command the configure the default current administrative value of actor state for the protocol partner.

Format	**no lacp partner admin state** *{individual|longtimeout|passive}*
Mode	Interface Config

lacp partner admin state individual

Use this command to set LACP partner admin state to individual.

Format	**lacp partner admin state individual**
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner admin state individual

Use this command to set the LACP partner admin state to aggregation.

Format	**no lacp partner admin state individual**
Mode	Interface Config

lacp partner admin state longtimeout

Use this command to set LACP partner admin state to longtimeout.

Format	**lacp partner admin state longtimeout**
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner admin state longtimeout

Use this command to set the LACP partner admin state to short timeout.

Format	**`no lacp partner admin state longtimeout`**
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

lacp partner admin state passive

Use this command to set the LACP partner admin state to passive.

Format	**`lacp partner admin state passive`**
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner admin state passive

Use this command to set the LACP partner admin state to active.

Format	**`no lacp partner admin state passive`**
Mode	Interface Config

lacp partner port id

Use this command to configure the LACP partner port id. The valid range for <*`port-id`*> is 0 to 65535.

Default	0x80
Format	**`lacp partner port-id`** *<port-id>*
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner port id

Use this command to set the LACP partner port id to the default.

Format	**`lacp partner port-id`**
Mode	Interface Config

lacp partner port priority

Use this command to configure the LACP partner port priority. The valid range for <*priority*> is 0 to 255.

Default	0x0
Format	**lacp partner port priority** <*priority*>
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner port priority

Use this command to configure the default LACP partner port priority.

Format	**no lacp partner port priority**
Mode	Interface Config

lacp partner system-id

Use this command to configure the 6-octet MAC Address value representing the administrative value of the Aggregation Port's protocol Partner's System ID. The valid range of <*system-id*> is 00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF.

Default	00:00:00:00:00:00
Format	**lacp partner system-id** <*system-id*>
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner system-id

Use this command to configure the default value representing the administrative value of the Aggregation Port's protocol Partner's System ID.

Format	**no lacp partner system-id**
Mode	Interface Config

lacp partner system priority

Use this command to configure the administrative value of the priority associated with the Partner's System ID. The valid range for <*priority*> is 0 to 255.

Default	0x0
Format	**lacp partner system priority** <*priority*>
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner system priority

Use this command to configure the default administrative value of priority associated with the Partner's System ID.

Format	`no lacp partner system priority`
Mode	Interface Config

port-channel static

This command enables the static mode on a port-channel (LAG) interface. By default the static mode for a new port-channel is disabled, which means the port-channel is dynamic. However if the maximum number of allowable dynamic port-channels are already present in the system, the static mode for a new port-channel enabled, which means the port-channel is static.You can only use this command on port-channel interfaces.

Default	disabled
Format	`port-channel static`
Mode	Interface Config

no port-channel static

This command sets the static mode on a particular port-channel (LAG) interface to the default value. This command will be executed only for interfaces of type port-channel (LAG).

Format	`no port-channel static`
Mode	Interface Config

port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port.

Default	enabled
Format	`port lacpmode`
Mode	Interface Config

no port lacpmode

This command disables Link Aggregation Control Protocol (LACP) on a port.

Format	`no port lacpmode`
Mode	Interface Config

port lacpmode all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Format	`port lacpmode all`
Mode	Global Config

no port lacpmode all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

Format	`no port lacpmode all`
Mode	Global Config

port lacptimeout (Interface Config)

This command sets the timeout on a physical interface of a particular device type (**actor** or **partner**) to either **long** or **short** timeout.

Default	long
Format	`port lacptimeout` *{actor | partner} {long | short}*
Mode	Interface Config

no port lacptimeout

This command sets the timeout back to its default value on a physical interface of a particular device type (**actor** or **partner**).

Format	`no port lacptimeout` *{actor | partner}*
Mode	Interface Config

port lacptimeout (Global Config)

This command sets the timeout for all interfaces of a particular device type (**actor** or **partner**) to either **long** or **short** timeout.

Default	long
Format	`port lacptimeout` *{actor | partner} {long | short}*
Mode	Global Config

Default	long
Format	`port lacptimeout` *{actor | partner} {long | short}*
Mode	Global Config

no port lacptimeout

This command sets the timeout for all physical interfaces of a particular device type (**actor** or **partner**) back to their default values.

Format	**no port lacptimeout** *{actor | partner}*
Mode	Global Config

port-channel adminmode

This command enables a port-channel (LAG). The option **all** sets every configured port-channel with the same administrative mode setting.

Format	**port-channel adminmode** *[all]*
Mode	Global Config

no port-channel adminmode

This command disables a port-channel (LAG). The option **all** sets every configured port-channel with the same administrative mode setting.

Format	**no port-channel adminmode** *[all]*
Mode	Global Config

port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a logical slot/port for a configured port-channel. The option **all** sets every configured port-channel with the same administrative mode setting.

Default	enabled
Format	**port-channel linktrap** *{<logical slot/port> | all}*
Mode	Global Config

no port-channel linktrap

This command disables link trap notifications for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option **all** sets every configured port-channel with the same administrative mode setting.

Format	**no port-channel linktrap** *{<logical slot/port> | all}*
Mode	Global Config

port-channel load-balance

This command selects the load-balancing option used on a port-channel (LAG). Traffic is balanced on a port-channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link.

Load-balancing is not supported on every device. The range of options for load-balancing may vary per device.

Default 3

Format **port-channel load-balance** *{1 | 2 | 3 | 4 | 5 | 6} {<slot/port> |<all>}*

Mode Interface Config
Global Config

Term	*Definition*
1	Source MAC, VLAN, EtherType, and incoming port associated with the packet
2	Destination MAC, VLAN, EtherType, and incoming port associated with the packet
3	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet
4	Source IP and Source TCP/UDP fields of the packet
5	Destination IP and Destination TCP/UDP Port fields of the packet
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet
<slot/port>| all	Global Config Mode only: The interface is a logical slot/port number of a configured port-channel. **All** applies the command to all currently configured port-channels.

no port-channel load-balance

This command reverts to the default load balancing configuration.

Format **no port-channel load-balance** *{<slot/port> | <all>}*

Mode Interface Config
Global Config

Term	*Definition*
<slot/port>| all	Global Config Mode only: The interface is a logical slot/port number of a configured port-channel. **All** applies the command to all currently configured port-channels.

port-channel name

This command defines a name for the port-channel (LAG). The interface is a logical slot/port for a configured port-channel, and *<name>* is an alphanumeric string up to 15 characters.

Format **port-channel name** *{<logical slot/port> | all | <name>}*

Mode Global Config

port-channel system priority

Use this command to configure port-channel system priority. The valid range of <priority> is 0-65535.

Default 0x8000

Format **port-channel system priority** *<priority>*

Mode Global Config

no port-channel system priority

Use this command to configure the default port-channel system priority value.

Format	**no port-channel system priority**
Mode	Global Config

show lacp actor

Use this command to display LACP actor attributes.

Format	**show lacp actor** *{<slot/port>|all}*
Mode	Global Config

The following output parameters are displayed.

Parameter	*Description*
System Priority	The administrative value of the Key.
Actor Admin Key	The administrative value of the Key.
Port Priority	The priority value assigned to the Aggregation Port.
Admin State	The administrative values of the actor state as transmitted by the Actor in LACPDUs.

show lacp partner

Use this command to display LACP partner attributes.

Format	**show lacp actor** *{<slot/port>|all}*
Mode	Privileged EXEC

The following output parameters are displayed.

Parameter	*Description*
System Priority	The administrative value of priority associated with the Partner's System ID.
System-ID	The value representing the administrative value of the Aggregation Port's protocol Partner's System ID.
Admin Key	The administrative value of the Key for the protocol Partner.
Port Priority	The administrative value of the Key for protocol Partner.
Port-ID	The administrative value of the port number for the protocol Partner.
Admin State	The administrative values of the actor state for the protocol Partner.

show port-channel brief

This command displays the static capability of all port-channel (LAG) interfaces on the device as well as a summary of individual port-channel interfaces.

Format `show port-channel brief`

Mode
- Privileged EXEC
- User EXEC

For each port-channel the following information is displayed:

Term	*Definition*
Logical Interface	The slot/port of the logical interface.
Port-channel Name	The name of port-channel (LAG) interface.
Link-State	Shows whether the link is up or down.
Trap Flag	Shows whether trap flags are enabled or disabled.
Type	Shows whether the port-channel is statically or dynamically maintained.
Mbr Ports	The members of this port-channel.
Active Ports	The ports that are actively participating in the port-channel.

show port-channel

This command displays an overview of all port-channels (LAGs) on the switch.

Format `show port-channel` *{<logical slot/port> | all}*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Logical Interface	Valid slot and port number separated by a forward slash.
Port-Channel Name	The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Type	The status designating whether a particular port-channel (LAG) is statically or dynamically maintained. • **Static** - The port-channel is statically maintained. • **Dynamic** - The port-channel is dynamically maintained.
Mbr Ports	A listing of the ports that are members of this port-channel (LAG), in slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).
Device Timeout	For each port, lists the timeout (**long** or **short**) for Device Type (**actor** or **partner**).
Port Speed	Speed of the port-channel port.
Active Ports	This field lists ports that are actively participating in the port-channel (LAG).
Load Balance Option	The load balance option associated with this LAG. See “port-channel load-balance” on page 90.

show port-channel system priority

Use this command to display the port-channel system priority.

Format	**show port-channel system priority**
Mode	Privileged EXEC

PORT MIRRORING

Port mirroring, which is also known as port monitoring, selects network traffic that you can analyze with a network analyzer, such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

monitor session

This command configures a probe port and a monitored port for monitor session (port monitoring). Use the *source interface <slot/port>* parameter to specify the interface to monitor. Use *rx* to monitor only ingress packets, or use *tx* to monitor only egress packets. If you do not specify an *{rx | tx}* option, the destination port monitors both ingress and egress packets. Use the *destination interface <slot/port>* to specify the interface to receive the monitored traffic. Use the *mode* parameter to enabled the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Format	**monitor session** *<session-id> {source interface <slot/port> [{rx | tx}] | destination interface <slot/port> | mode}*
Mode	Global Config

no monitor session

Use this command without optional parameters to remove the monitor session (port monitoring) designation from the source probe port, the destination monitored port and all VLANs. Once the port is removed from the VLAN, you must manually add the port to any desired VLANs. Use the *source interface <slot/port>* parameter or *destination interface <slot/port>* to remove the specified interface from the port monitoring session. Use the *mode* parameter to disable the administrative mode of the session.

Note: Since the current version of Unified Switch software only supports one session, if you do not supply optional parameters, the behavior of this command is similar to the behavior of the **no monitor** command.

Format	**no monitor session** *<session-id> [{source interface <slot/port> | destination interface <slot/port> | mode}]*
Mode	Global Config

no monitor

This command removes all the source ports and a destination port for the and restores the default value for mirroring session mode for all the configured sessions.

Note: This is a stand-alone “no” command. This command does not have a “normal” form.

Default enabled

Format `no monitor`

Mode Global Config

show monitor session

This command displays the Port monitoring information for a particular mirroring session.

Note: The *<session-id>* parameter is an integer value used to identify the session. In the current version of the software, the *<session-id>* parameter is always one (1).

Format `show monitor session` *<session-id>*

Mode Privileged EXEC

Term	*Definition*
Session ID	An integer value used to identify the session. Its value can be anything between 1 and the maximum number of mirroring sessions allowed on the platform.
Monitor Session Mode	Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with *<session-id>*. The possible values are Enabled and Disabled.
Probe Port	Probe port (destination port) for the session identified with *<session-id>*. If probe port is not set then this field is blank.
Source Port	The port, which is configured as mirrored port (source port) for the session identified with *<session-id>*. If no source port is configured for the session then this field is blank.
Type	Direction in which source port configured for port mirroring.Types are tx for transmitted packets and rx for receiving packets.

STATIC MAC FILTERING

The commands in this section describe how to configure static MAC filtering. Static MAC filtering allows you to configure destination ports for a static multicast MAC filter irrespective of the platform.

macfilter

This command adds a static MAC filter entry for the MAC address *<macaddr>* on the VLAN *<vlanid>*. The value of the *<macaddr>* parameter is a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The restricted MAC Addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF. The *<vlanid>* parameter must identify a valid VLAN.

The number of static mac filters supported on the system is different for MAC filters where source ports are configured and MAC filters where destination ports are configured.

- For unicast MAC address filters and multicast MAC address filters with source port lists, the maximum number of static MAC filters supported is 20.
- For multicast MAC address filters with destination ports configured, the maximum number of static filters supported is 256.

You can configure the following combinations:

- Unicast MAC and source port (max = 20)
- Multicast MAC and source port (max = 20)
- Multicast MAC and destination port (only) (max = 256)
- Multicast MAC and source ports and destination ports (max = 20)

Format	**macfilter** *<macaddr> <vlanid>*
Mode	Global Config

no macfilter

This command removes all filtering restrictions and the static MAC filter entry for the MAC address *<macaddr>* on the VLAN *<vlanid>*. The *<macaddr>* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The *<vlanid>* parameter must identify a valid VLAN.

Format	**no macfilter** *<macaddr> <vlanid>*
Mode	Global Config

macfilter adddest

Use this command to add the interface to the destination filter set for the MAC filter with the given *<macaddr>* and VLAN of *<vlanid>*. The *<macaddr>* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Note: Configuring a destination port list is only valid for multicast MAC addresses.

Format	**macfilter adddest <***macaddr***>**
Mode	Interface Config

no macfilter adddest

This command removes a port from the destination filter set for the MAC filter with the given *<macaddr>* and VLAN of *<vlanid>*. The *<macaddr>* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Format	**no macfilter adddest** *<macaddr>*
Mode	Interface Config

macfilter adddest all

This command adds all interfaces to the destination filter set for the MAC filter with the given *<macaddr>* and VLAN of *<vlanid>*. The *<macaddr>* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Note: Configuring a destination port list is only valid for multicast MAC addresses.

Format	**macfilter adddest all** *<macaddr>*
Mode	Global Config

no macfilter adddest all

This command removes all ports from the destination filter set for the MAC filter with the given *<macaddr>* and VLAN of *<vlanid>*. The *<macaddr>* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Format	**no macfilter adddest all** *<macaddr>*
Mode	Global Config

macfilter addsrc

This command adds the interface to the source filter set for the MAC filter with the MAC address of <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Format	**macfilter addsrc** *<macaddr> <vlanid>*
Mode	Interface Config

no macfilter addsrc

This command removes a port from the source filter set for the MAC filter with the MAC address of *<macaddr>* and VLAN of *<vlanid>*. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Format	**no macfilter addsrc** *<macaddr> <vlanid>*
Mode	Interface Config

macfilter addsrc all

This command adds all interfaces to the source filter set for the MAC filter with the MAC address of *<macaddr>* and *<vlanid>*. You must specify the *<macaddr>* parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Format	**macfilter addsrc all** *<macaddr> <vlanid>*
Mode	Global Config

no macfilter addsrc all

This command removes all interfaces to the source filter set for the MAC filter with the MAC address of *<macaddr>* and VLAN of *<vlanid>*. You must specify the *<macaddr>* parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The *<vlanid>* parameter must identify a valid VLAN.

Format	**no macfilter addsrc all** *<macaddr> <vlanid>*
Mode	Global Config

show mac-address-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If you select *<all>*, all the Static MAC Filters in the system are displayed. If you supply a value for *<macaddr>,* you must also enter a value for *<vlanid>*, and the system displays Static MAC Filter information only for that MAC address and VLAN.

Format	**show mac-address-table static** *{<macaddr> <vlanid> | all}*
Mode	Privileged EXEC

Term	*Definition*
MAC Address	The MAC Address of the static MAC filter entry.
VLAN ID	The VLAN ID of the static MAC filter entry.
Source Port(s)	The source port filter set's slot and port(s).

Note: Only multicast address filters will have destination port lists.

show mac-address-table staticfiltering

This command displays the Static Filtering entries in the Multicast Forwarding Database (MFDB) table.

Format	**show mac-address-table staticfiltering**
Mode	Privileged EXEC

Term	*Definition*
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. As the data is gleaned from the MFDB, the address will be a multicast address. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

L2 DHCP Relay Agent Commands

You can enable the switch to operate as a Layer 2 DHCP relay agent to relay DHCP requests from clients to a Layer 3 relay agent or server. The Circuit ID and Remote ID can be added to DHCP requests relayed from clients to a DHCP server. This information is included in DHCP Option 82, as specified in sections 3.1 and 3.2 of RFC3046.

dhcp l2relay

This command enables the Layer 2 DHCP Relay agent for an interface. The subsequent commands mentioned in this section can only be used when the L2 DHCP relay is enabled.

Format `dhcp l2relay`

Mode
- Global Config
- Interface Config

no dhcp l2relay

This command disables Layer 2 DHCP relay agent for an interface.

Format `no dhcp l2relay`

Mode
- Global Config
- Interface Config

dhcp l2relay circuit-id vlan

This parameter sets the DHCP Option-82 Circuit ID for a VLAN. When enabled, the interface number is added as the Circuit ID in DHCP option 82.

Format `dhcp l2relay circuit-id vlan` *<vlan-range>*

Mode Global Config

no dhcp l2relay circuit-id vlan

This parameter clears the DHCP Option-82 Circuit ID for a VLAN.

Format `no dhcp l2relay circuit-id vlan` *<vlan-range>*

Mode Global Config

dhcp l2relay remote-id vlan

This parameter sets the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format `dhcp l2relay remote-id` *<remote-id-string>* `vlan` *<vlan-range>*

Mode Global Config

no dhcp l2relay remote-id vlan

This parameter clears the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format	**no dhcp l2relay remote-id** vlan <*vlan-range*>
Mode	Global Config

dhcp l2relay trust

Use this command to configure an interface as trusted for Option-82 reception.

Default	untrusted
Format	**dhcp l2relay trust**
Mode	Interface Config

no dhcp l2relay trust

Use this command to configure an interface to the default untrusted for Option-82 reception.

Format	**no dhcp l2relay trust**
Mode	Interface Config

dhcp l2relay vlan

Use this command to enable the L2 DHCP Relay agent for a set of VLANs. All DHCP packets which arrive on interfaces in the configured VLAN are subject to L2 Relay processing.

Default	disable
Format	**dhcp l2relay vlan** <vlan-range>
Mode	Global Config

no dhcp l2relay vlan

Use this command to disable the L2 DHCP Relay agent for a set of VLANs.

Format	**no dhcp l2relay vlan** <vlan-range>
Mode	Global Config

show dhcp l2relay all

This command displays the summary of DHCP L2 Relay configuration.

Format	show dhcp l2relay all
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show dhcp l2relay all

DHCP L2 Relay is  Enabled.

Interface  L2RelayMode   TrustMode
---------  -----------  --------------
 0/2        Enabled      untrusted
 0/4        Disabled     trusted

VLAN Id    L2 Relay   CircuitId   RemoteId
-------- ----------  ----------- ------------
 3          Disabled    Enabled    --NULL--
 4          Disabled    Enabled    EnterpriseSwitch
 5          Enabled     Enabled    --NULL--
 6          Enabled     Enabled    EnterpriseSwitch
 7          Enabled     Disabled   --NULL--
 8          Enabled     Disabled   --NULL--
 9          Enabled     Disabled   --NULL--
 10         Enabled     Disabled   --NULL--
```

show dhcp l2relay interface

This command displays DHCP L2 relay configuration specific to interfaces.

Format `show dhcp l2relay interface {all|<interface-num>}`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show dhcp l2relay interface all

DHCP L2 Relay is  Enabled.

Interface  L2RelayMode   TrustMode
---------  -----------  --------------
 0/2        Enabled      untrusted
 0/4        Disabled     trusted
```

show dhcp l2relay stats interface

This command displays statistics specific to DHCP L2 Relay configured interface.

Format `show dhcp l2relay stats interface {all|<interface-num>}`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show dhcp l2relay stats interface all

DHCP L2 Relay is  Enabled.

Interface  UntrustedServer    UntrustedClient  TrustedServer     TrustedClient
           MsgsWithOpt82    MsgsWithOpt82    MsgsWithoutOpt82  MsgsWithoutOpt82
```

```
---------  --------------- -----------------  ----------------- --------------
 0/1            0                 0                 0                0
 0/2            0                 0                 3                7
 0/3            0                 0                 0                0
 0/4            0                 12                0                0
 0/5            0                 0                 0                0
 0/6            3                 0                 0                0
 0/7            0                 0                 0                0
 0/8            0                 0                 0                0
 0/9            0                 0                 0                0
```

show dhcp l2relay agent-option vlan

This command displays the DHCP L2 Relay Option-82 configuration specific to VLAN.

Format `show dhcp l2relay agent-option vlan <vlan-range>`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show dhcp l2relay agent-option vlan 5-10

DHCP L2 Relay is  Enabled.

VLAN Id    L2 Relay  CircuitId  RemoteId
--------- ----------  ----------- ------------
5           Enabled     Enabled    --NULL--
6           Enabled     Enabled    EnterpriseSwitch
7           Enabled     Disabled   --NULL--
8           Enabled     Disabled   --NULL--
9           Enabled     Disabled   --NULL--
10          Enabled     Disabled   --NULL--
```


show dhcp l2relay vlan

This command shows whether DHCP L2 Relay is enabled globally and on a particular VLAN or range of VLANs.

Format `show dhcp l2relay vlan <vlan-range>`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show dhcp l2relay vlan 1-2

DHCP L2 Relay is  Enabled.

DHCP L2 Relay is enabled on the following VLANs:
2
```

show dhcp l2relay circuit-id vlan

This command shows whether DHCP L2 Relay is enabled globally and shows the VLANs for which the Circuit ID option is enabled. When the Circuit ID option is enabled for a VLAN, the interface number is added as the Circuit ID in DHCP option 82.

Format `show dhcp l2relay circuit-id vlan <vlan-range>`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) ##show dhcp l2relay circuit-id vlan 1-3

DHCP L2 Relay is  Enabled.

DHCP Circuit-Id option is enabled on the following VLANs:
2 - 3
```

show dhcp l2relay remote-id vlan

This command shows whether DHCP L2 Relay is enabled globally and shows the remote ID associated with each VLAN on which DHCP relay is enabled. The DHCP Option-82 Remote ID identifies a trusted identifier for the remote device.

Format `show dhcp l2relay remote-id vlan <vlan-range>`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show dhcp l2relay remote-id vlan 1-3

DHCP L2 Relay is  Enabled.

VLAN ID    Remote Id
---------  -------------
2          20
3          30
```

DHCP CLIENT COMMANDS

Unified Switch can include vendor and configuration information in DHCP client requests relayed to a DHCP server. This information is included in DHCP Option 60, Vendor Class Identifier. The information is a string of 128 octets.

dhcp client vendor-id-option

This command enables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the Unified Switch switch.

Format	**dhcp client vendor-id-option** *<string>*
Mode	Global Config

no dhcp client vendor-id-option

This command disables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the Unified Switch switch.

Format	**no dhcp client vendor-id-option**
Mode	Global Config

dhcp client vendor-id-option-string

This parameter sets the DHCP Vendor Option-60 string to be included in the requests transmitted to the DHCP server by the DHCP client operating in the Unified Switch switch.

Format	**dhcp client vendor-id-option-string** *<string>*
Mode	Global Config

no dhcp client vendor-id-option-string

This parameter clears the DHCP Vendor Option-60 string.

Format	**no dhcp client vendor-id-option-string**
Mode	Global Config

show dhcp client vendor-id-option

This command displays the configured administration mode of the vendor-id-option and the vendor-id string to be included in Option-43 in DHCP requests.

Format	**show dhcp client vendor-id-option**
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show dhcp client vendor-id-option

DHCP Client Vendor Identifier Option is Enabled
DHCP Client Vendor Identifier Option string is D-LinkClient.
```

DHCP SNOOPING CONFIGURATION COMMANDS

This section describes commands you use to configure DHCP Snooping.

ip dhcp snooping

Use this command to enable DHCP Snooping globally.

Default	disabled
Format	**`ip dhcp snooping`**
Mode	Global Config

no ip dhcp snooping

Use this command to disable DHCP Snooping globally.

Format	**`no ip dhcp snooping`**
Mode	Global Config

ip dhcp snooping vlan

Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

Default	disabled
Format	**`ip dhcp snooping vlan <vlan-list>`**
Mode	Global Config

no ip dhcp snooping vlan

Use this command to disable DHCP Snooping on VLANs.

Format	**`no ip dhcp snooping vlan <vlan-list>`**
Mode	Global Config

ip dhcp snooping verify mac-address

Use this command to enable verification of the source MAC address with the client hardware address in the received DCHP message.

Default	enabled
Format	`ip dhcp snooping verify mac-address`
Mode	Global Config

no ip dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

Format	`no ip dhcp snooping verify mac-address`
Mode	Global Config

ip dhcp snooping database

Use this command to configure the persistent location of the DHCP Snooping database. This can be local or a remote file on a given IP machine.

Default	local
Format	`ip dhcp snooping database {local|tftp://hostIP/filename}`
Mode	Global Config

ip dhcp snooping database write-delay

Use this command to configure the interval in seconds at which the DHCP Snooping database will be persisted. The interval value ranges from 15 to 86400 seconds.

Default	300 seconds
Format	`ip dhcp snooping database write-delay <in seconds>`
Mode	Global Config

no ip dhcp snooping database write-delay

Use this command to set the write delay value to the default value.

Format	`no ip dhcp snooping database write-delay`
Mode	Global Config

ip dhcp snooping binding

Use this command to configure static DHCP Snooping binding.

Format	`ip dhcp snooping binding <mac-address> vlan <vlan id> <ip address> interface <interface id>`
Mode	Global Config

no ip dhcp snooping binding **<mac-address>**

Use this command to remove the DHCP static entry from the DHCP Snooping database.

Format	**no ip dhcp snooping binding <mac-address>**
Mode	Global Config

ip verify binding

Use this command to configure static IP source guard (IPSG) entries.

Format	**ip verify binding <mac-address> vlan <vlan id> <ip address> interface <interface id>**
Mode	Global Config

no ip verify binding

Use this command to remove the IPSG static entry from the IPSG database.

Format	**no ip verify binding <mac-address> vlan <vlan id> <ip address> interface <interface id>**
Mode	Global Config

ip dhcp snooping limit

Use this command to control the rate at which the DHCP Snooping messages come. The default rate is 15 pps with a range from 0 to 30 pps. The default burst level is 1 second with a range of 1 to 15 seconds.

Default	15 pps for rate limiting and 1 sec for burst interval
Format	**ip dhcp snooping limit {rate pps [burst interval seconds]}**
Mode	Interface Config

no ip dhcp snooping limit

Use this command to set the rate at which the DHCP Snooping messages come, and the burst level, to the defaults.

Format	**no ip dhcp snooping limit**
Mode	Interface Config

ip dhcp snooping log-invalid

Use this command to control the logging DHCP messages filtration by the DHCP Snooping application.

Default	disabled
Format	**ip dhcp snooping log-invalid**
Mode	Interface Config

no ip dhcp snooping log-invalid

Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

Format	`no ip dhcp snooping log-invalid`
Mode	Interface Config

ip dhcp snooping trust

Use this command to configure the port as trusted.

Default	disabled
Format	`ip dhcp snooping trust`
Mode	Interface Config

no ip dhcp snooping trust

Use this command to configure the port as untrusted.

Format	`no ip dhcp snooping trust`
Mode	Interface Config

ip verify source

Use this command to configure the IPSG source ID attribute to filter the data traffic in the hardware. Source ID is the combination of IP address and MAC address. Normal command allows data traffic filtration based on the IP address. With the “port-security” option, the data traffic will be filtered based on the IP and MAC addresses.

Default	`the source ID is the IP address`
Format	`ip verify source {port-security}`
Mode	Interface Config

no ip verify source

Use this command to disable the IPSG configuration in the hardware. You cannot disable port-security alone if it is configured.

Format	`no ip verify source`
Mode	Interface Config

show ip dhcp snooping

Use this command to display the DHCP Snooping global configurations and per port configurations.

Format	`show ip dhcp snooping`
Mode	• Privileged EXEC • User EXEC

Term	*Definition*
Interface	The interface for which data is displayed.
Trusted	If it is enabled, DHCP snooping considers the port as trusted. The factory default is disabled.
Log Invalid Pkts	If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show ip dhcp snooping

DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
11 - 30, 40

Interface   Trusted    Log Invalid Pkts
---------   --------   ----------------
0/1          Yes             No
0/2          No             Yes
0/3          No             Yes
0/4          No              No
0/6          No              No
```

show ip dhcp snooping binding

Use this command to display the DHCP Snooping binding entries. To restrict the output, use the following options:

- Dynamic: Restrict the output based on DCHP snooping.
- Interface: Restrict the output based on a specific interface.
- Static: Restrict the output based on static entries.
- VLAN: Restrict the output based on VLAN.

Format **show ip dhcp snooping binding** *[{static/dynamic}] [interface slot/port] [vlan id]*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
MAC Address	Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.
IP Address	Displays the valid IP address for the binding rule.
VLAN	The VLAN for the binding rule.
Interface	The interface to add a binding into the DHCP snooping interface.
Type	Binding type; statically configured from the CLI or dynamically learned.
Lease (sec)	The remaining lease time for the entry.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show ip dhcp snooping binding
```

```
Total number of bindings: 2

MAC Address          IP Address   VLAN  Interface  Type  Lease (Secs)
-----------------  ------------  ----  ---------  ---- -------------
00:02:B3:06:60:80   210.1.1.3      10   0/1           86400
00:0F:FE:00:13:04   210.1.1.4      10   0/1           86400
```

show ip dhcp snooping database

Use this command to display the DHCP Snooping configuration related to the database persistency.

Format `show ip dhcp snooping database`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Agent URL	Bindings database agent URL.
Write Delay	The maximum write time to write the database into local or remote.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show ip dhcp snooping database

agent url:  /10.131.13.79:/sai1.txt

write-delay:  5000
```

show ip dhcp snooping statistics

Use this command to list statistics for DHCP Snooping security violations on untrusted ports.

Format `show ip dhcp snooping statistics`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	The IP address of the interface in slot/port format.
MAC Verify Failures	Represents the number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client HW address mismatch.
Client Ifc Mismatch	Represents the number of DHCP release and Deny messages received on the different ports than learned previously.
DHCP Server Msgs Rec'd	Represents the number of DHCP server messages received on Untrusted ports.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show ip dhcp snooping statistics

 Interface    MAC Verify   Client Ifc   DHCP Server
              Failures     Mismatch     Msgs Rec'd
```



```
-----------   ----------   ----------   -----------
0/2                    0            0             0
0/3                    0            0             0
0/4                    0            0             0
0/5                    0            0             0
0/6                    0            0             0
0/7                    0            0             0
0/8                    0            0             0
0/9                    0            0             0
0/10                   0            0             0
0/11                   0            0             0
0/12                   0            0             0
0/13                   0            0             0
0/14                   0            0             0
0/15                   0            0             0
0/16                   0            0             0
0/17                   0            0             0
0/18                   0            0             0
0/19                   0            0             0
0/20                   0            0             0
```

clear ip dhcp snooping binding

Use this command to clear all DHCP Snooping bindings on all interfaces or on a specific interface.

Format `clear ip dhcp snooping binding` *[interface <slot/port>]*

Mode
- Privileged EXEC
- User EXEC

clear ip dhcp snooping statistics

Use this command to clear all DHCP Snooping statistics.

Format `clear ip dhcp snooping statistics`

Mode
- Privileged EXEC
- User EXEC

show ip verify source

Use this command to display the IPSG configurations on all ports.

Format `show ip verify source`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Interface address in slot/port format.
Filter Type	Is one of two values: • ip-mac: User has configured MAC address filtering on this interface. • ip: Only IP address filtering on this interface.

Term	*Definition*
IP Address	IP address of the interface
MAC Address	If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, then the MAC Address field displays “permit-all.”
VLAN	The VLAN for the binding rule.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show ip verify source

Interface  Filter Type    IP Address       MAC Address       Vlan
---------  -----------  ---------------  -----------------  -----
    0/1     ip-mac       210.1.1.3       00:02:B3:06:60:80     10
    0/1     ip-mac       210.1.1.4       00:0F:FE:00:13:04     10
```

show ip source binding

Use this command to display the IPSG bindings.

Format **`show ip source binding`** *`[{static/dynamic}] [interface slot/port] [vlan id]`*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
MAC Address	The MAC address for the entry that is added.
IP Address	The IP address of the entry that is added.
Type	Entry type; statically configured from CLI or dynamically learned from DHCP Snooping.
VLAN	VLAN for the entry.
Interface	IP address of the interface in slot/port format.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show ip source binding

MAC Address       IP Address       Type         Vlan     Interface
----------------  ---------------  -------------  -----  -------------
00:00:00:00:00:08          1.2.3.4  dhcp-snooping     2         0/1

00:00:00:00:00:09          1.2.3.4  dhcp-snooping     3         0/1

00:00:00:00:00:0A          1.2.3.4  dhcp-snooping     4         0/1
```

DYNAMIC ARP INSPECTION COMMANDS

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of

its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid {MAC address, IP address, VLAN, and interface} tuples.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

ip arp inspection vlan

Use this command to enable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Default	`disabled`
Format	**`ip arp inspection vlan vlan-list`**
Mode	Global Config

no ip arp inspection vlan

Use this command to disable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Format	**`no ip arp inspection vlan vlan-list`**
Mode	Global Config

ip arp inspection validate

Use this command to enable additional validation checks like source-mac validation, destination-mac validation, and ip address validation on the received ARP packets. Each command overrides the configuration of the previous command. For example, if a command enables src-mac and dst-mac validations, and a second command enables IP validation only, the src-mac and dst-mac validations are disabled as a result of the second command.

Default	`disabled`
Format	**`ip arp inspection validate {[src-mac] [dst-mac] [ip]}`**
Mode	Global Config

no ip arp inspection validate

Use this command to disable the additional validation checks on the received ARP packets.

Format	**`no ip arp inspection validate {[src-mac] [dst-mac] [ip]}`**
Mode	Global Config

ip arp inspection vlan logging

Use this command to enable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Default	enabled
Format	**ip arp inspection vlan vlan-list logging**
Mode	Global Config

no ip arp inspection vlan logging

Use this command to disable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Format	**no ip arp inspection vlan vlan-list logging**
Mode	Global Config

ip arp inspection trust

Use this command to configure an interface as trusted for Dynamic ARP Inspection.

Default	enabled
Format	**ip arp inspection trust**
Mode	Interface Config

no ip arp inspection trust

Use this command to configure an interface as untrusted for Dynamic ARP Inspection.

Format	**no ip arp inspection trust**
Mode	Interface Config

ip arp inspection limit

Use this command to configure the rate limit and burst interval values for an interface. Configuring none for the limit means the interface is not rate limited for Dynamic ARP Inspections.

Note: The user interface will accept a rate limit for a trusted interface, but the limit will not be enforced unless the interface is configured to be untrusted.

Default	15 pps for rate and 1 second for burst-interval
Format	**ip arp inspection limit {rate pps [burst interval seconds] | none}**
Mode	Interface Config

no ip arp inspection limit

Use this command to set the rate limit and burst interval values for an interface to the default values of 15 pps and 1 second, respectively.

Format	**no ip arp inspection limit**
Mode	Interface Config

ip arp inspection filter

Use this command to configure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges. If the static keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings.

Default	`No ARP ACL is configured on a VLAN`
Format	**`ip arp inspection filter acl-name vlan vlan-list [static]`**
Mode	Global Config

no ip arp inspection filter

Use this command to unconfigure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges.

Format	**`no ip arp inspection filter acl-name vlan vlan-list [static]`**
Mode	Global Config

arp access-list

Use this command to create an ARP ACL.

Format	**`arp access-list acl-name`**
Mode	Global Config

no arp access-list

Use this command to delete a configured ARP ACL.

Format	**`no arp access-list acl-name`**
Mode	Global Config

permit ip host mac host

Use this command to configure a rule for a valid IP address and MAC address combination used in ARP packet validation.

Format	**`permit ip host sender-ip mac host sender-mac`**
Mode	ARP Access-list Config

no permit ip host mac host

Use this command to delete a rule for a valid IP and MAC combination.

Format	**`no permit ip host sender-ip mac host sender-mac`**
Mode	ARP Access-list Config

show ip arp inspection

Use this command to display the Dynamic ARP Inspection global configuration and configuration on all the VLANs. With the *vlan-list* argument (i.e. comma separated VLAN ranges), the command displays the global configuration and configuration on all the VLANs in the given VLAN list. The global configuration includes the **source mac validation**, **destination mac validation** and **invalid IP validation** information.

Format `show ip arp inspection [vlan <vlan-list>]`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Source MAC Validation	Displays whether Source MAC Validation of ARP frame is enabled or disabled.
Destination MAC Validation	Displays whether Destination MAC Validation is enabled or disabled.
IP Address Validation	Displays whether IP Address Validation is enabled or disabled.
VLAN	The VLAN ID for each displayed row.
Configuration	Displays whether DAI is enabled or disabled on the VLAN.
Log Invalid	Displays whether logging of invalid ARP packets is enabled on the VLAN.
ACL Name	The ARP ACL Name, if configured on the VLAN.
Static Flag	If the ARP ACL is configured static on the VLAN.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show ip arp inspection vlan 10-12

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan          Configuration    Log Invalid   ACL Name   Static flag
 ----          -------------    -----------   ---------  ----------
   10               Enabled        Enabled   H2         Enabled
   11              Disabled        Enabled
   12              Enabled        Disabled
```

show ip arp inspection statistics

Use this command to display the statistics of the ARP packets processed by Dynamic ARP Inspection. Give the vlan-list argument and the command displays the statistics on all DAI-enabled VLANs in that list. Give the single vlan argument and the command displays the statistics on that VLAN. If no argument is included, the command lists a summary of the forwarded and dropped ARP packets.

Format `show ip arp inspection statistics [vlan vlan-list]`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
VLAN	The VLAN ID for each displayed row.
Forwarded	The total number of valid ARP packets forwarded in this VLAN.
Dropped	The total number of not valid ARP packets dropped in this VLAN.
DHCP Drops	The number of packets dropped due to DHCP snooping binding database match failure.
ACL Drops	The number of packets dropped due to ARP ACL rule match failure.
DHCP Permits	The number of packets permitted due to DHCP snooping binding database match.
ACL Permits	The number of packets permitted due to ARP ACL rule match.
Bad Src MAC	The number of packets dropped due to Source MAC validation failure.
Bad Dest MAC	The number of packets dropped due to Destination MAC validation failure.
Invalid IP	The number of packets dropped due to invalid IP checks.

Example: The following shows example CLI display output for the command **show ip arp inspection statistics** which lists the summary of forwarded and dropped ARP packets on all DAI-enabled VLANs.

```
VLAN  Forwarded  Dropped
----  ---------  -------
  10         90       14
  20         10        3
```

Example: The following shows example CLI display output for the command **show ip arp inspection statistics vlan <*vlan-list*>**.

```
VLAN    DHCP       ACL        DHCP        ACL        Bad Src    Bad Dest    Invalid
         Drops     Drops       Permits     Permits     MAC        MAC         IP
----- -------- --------- ----------- --------- ---------- ----------- ---------
10       11         1            65          25          1          1          0
20       1          0             8           2          0          1          1
```

clear ip arp inspection statistics

Use this command to reset the statistics for Dynamic ARP Inspection on all VLANs.

Default `none`

Format `clear ip arp inspection statistics`

Mode Privileged EXEC

show ip arp inspection interfaces

Use this command to display the Dynamic ARP Inspection configuration on all the DAI-enabled interfaces. An interface is said to be enabled for DAI if at least one VLAN, that the interface is a member of, is enabled for DAI. Given a slot/port interface argument, the command displays the values for that interface whether the interface is enabled for DAI or not.

Format `show ip arp inspection interfaces [slot/port]`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	The interface ID for each displayed row.
Trust State	Whether the interface is trusted or untrusted for DAI.
Rate Limit	The configured rate limit value in packets per second.
Burst Interval	The configured burst interval value in seconds.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show ip arp inspection interfaces

 Interface        Trust State    Rate Limit   Burst Interval
                                    (pps)        (seconds)
 ---------------  -----------    ----------   ---------------
 0/1                Untrusted           15                1
 0/2                Untrusted           10               10
```

show arp access-list

Use this command to display the configured ARP ACLs with the rules. Giving an ARP ACL name as the argument will display only the rules in that ARP ACL.

Format `show arp access-list [acl-name]`

Mode
- Privileged EXEC
- User EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show arp access-list

ARP access list H2
    permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
    permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
ARP access list H3
ARP access list H4
    permit ip host 2.1.1.2 mac host 00:03:04:05:06:08
```


IGMP SNOOPING CONFIGURATION COMMANDS

This section describes the commands you use to configure IGMP snooping. Unified Switch software supports IGMP Versions 1, 2, and 3. The IGMP snooping feature can help conserve bandwidth because it allows the switch to forward IP multicast traffic only to connected hosts that request multicast traffic. IGMPv3 adds source filtering capabilities to IGMP versions 1 and 2.

set igmp

This command enables IGMP Snooping on the system (Global Config Mode) or an interface (Interface Config Mode). This command also enables IGMP snooping on a particular VLAN (VLAN Config Mode) and can enable IGMP snooping on all interfaces participating in a VLAN.

If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

The IGMP application supports the following activities:

- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default disabled

Format `set igmp`

Mode
- Global Config
- Interface Config

Format `set igmp` *<vlanid>*

Mode VLAN Config

no set igmp

This command disables IGMP Snooping on the system, an interface or a VLAN.

Format `no set igmp`

Mode
- Global Config
- Interface Config

Format `no set igmp` *<vlanid>*

Mode VLAN Config

set igmp interfacemode

This command enables IGMP Snooping on all interfaces. If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that

interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

Default	disabled
Format	**set igmp interfacemode**
Mode	Global Config

no set igmp interfacemode

This command disables IGMP Snooping on all interfaces.

Format	**no set igmp interfacemode**
Mode	Global Config

set igmp fast-leave

This command enables or disables IGMP Snooping fast-leave admin mode on a selected interface or VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

Default	disabled
Format	**set igmp fast-leave**
Mode	Interface Config

Format	**set igmp fast-leave** *<vlan_id>*
Mode	VLAN Config

no set igmp fast-leave

This command disables IGMP Snooping fast-leave admin mode on a selected interface.

Format	**no set igmp fast-leave**
Mode	Interface Config

Format	**no set igmp fast-leave** *<vlan_id>*
Mode	VLAN Config

set igmp groupmembership-interval

This command sets the IGMP Group Membership Interval time on a VLAN, one interface or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a

particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

Default 260 seconds

Format **set igmp groupmembership-interval** *<2-3600>*

Mode
- Interface Config
- Global Config

Format **set igmp groupmembership-interval** *<vlan_id> <2-3600>*

Mode VLAN Config

no set igmp groupmembership-interval

This command sets the IGMPv3 Group Membership Interval time to the default value.

Format **no set igmp groupmembership-interval**

Mode
- Interface Config
- Global Config

Format **no set igmp groupmembership-interval** *<vlan_id>*

Mode VLAN Config

set igmp maxresponse

This command sets the IGMP Maximum Response time for the system, or on a particular interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds.

Default 10 seconds

Format **set igmp maxresponse** *<1-25>*

Mode
- Global Config
- Interface Config

Format **set igmp maxresponse** *<vlan_id> <1-25>*

Mode VLAN Config

no set igmp maxresponse

This command sets the max response time (on the interface or VLAN) to the default value.

Format **no set igmp maxresponse**

Mode
- Global Config
- Interface Config

Format **no set igmp maxresponse** *<vlan_id>*
Mode VLAN Config

set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out, i.e. no expiration.

Default 0
Format **set igmp mcrtrexpiretime** *<0-3600>*
Mode
- Global Config
- Interface Config

Format **set igmp mcrtrexpiretime** *<vlan_id> <0-3600>*
Mode VLAN Config

no set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format **no set igmp mcrtrexpiretime**
Mode
- Global Config
- Interface Config

Format **no set igmp mcrtrexpiretime** *<vlan_id>*
Mode VLAN Config

set igmp mrouter

This command configures the VLAN ID (*<vlanId>*) that has the multicast router mode enabled.

Format **set igmp mrouter <***vlan_id***>**
Mode Interface Config

no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID (*<vlan_id>*).

Format **no set igmp mrouter <***vlan_id***>**
Mode Interface Config

set igmp mrouter interface

This command configures the interface as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs.

Default	disabled
Format	`set igmp mrouter interface`
Mode	Interface Config

no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

Format	`no set igmp mrouter interface`
Mode	Interface Config

show igmpsnooping

This command displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled.

Format	**`show igmpsnooping`** *[<slot/port> | <vlan_id>]*
Mode	Privileged EXEC

When the optional arguments *<slot/port>* or *<vlan_id>* are not used, the command displays the following information:

Term	*Definition*
Admin Mode	Indicates whether or not IGMP Snooping is active on the switch.
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interface Enabled for IGMP Snooping	The list of interfaces on which IGMP Snooping is enabled.
VLANS Enabled for IGMP Snooping	The list of VLANS on which IGMP Snooping is enabled.

When you specify the *<slot/port>* values, the following information appears:

Term	*Definition*
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the interface.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the interface.
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry.This value may be configured.
Maximum Response Time	The amount of time the switch waits after it sends a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time	The amount of time to wait before removing an interface from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for *<vlan_id>*, the following information appears:

Term	*Definition*
VLAN ID	The VLAN ID.
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the VLAN.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the VLAN.
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry.This value may be configured.
Maximum Response Time	The amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time	The amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

show igmpsnooping mrouter interface

This command displays information about statically configured ports.

Format **show igmpsnooping mrouter interface** *<slot/port>*

Mode Privileged EXEC

Term	*Definition*
Interface	The port on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	The list of VLANs of which the interface is a member.

show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

Format **show igmpsnooping mrouter vlan** *<slot/port>*

Mode Privileged EXEC

Term	*Definition*
Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the MFDB table.

Format `show mac-address-table igmpsnooping`

Mode Privileged EXEC

Term	*Definition*
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address is displayed as a MAC address and VLAN ID combination of 8 bytes.
Type	The type of the entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol).
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

IGMP SNOOPING QUERIER COMMANDS

IGMP Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the “IGMP Querier”. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes commands used to configure and display information on IGMP Snooping Queriers on the network and, separately, on VLANs.

set igmp querier

Use this command to enable IGMP Snooping Querier on the system, using Global Config mode, or on a VLAN. Using this command, you can specify the IP Address that the Snooping Querier switch should use as the source address while generating periodic queries.

If a VLAN has IGMP Snooping Querier enabled and IGMP Snooping is operationally disabled on it, IGMP Snooping Querier functionality is disabled on that VLAN. IGMP Snooping functionality is re-enabled if IGMP Snooping is operational on the VLAN.

Note: The Querier IP Address assigned for a VLAN takes preference over global configuration.

The IGMP Snooping Querier application supports sending periodic general queries on the VLAN to solicit membership reports.

Default disabled

Format `set igmp querier [<vlan-id>] [address ipv4_address]`

Mode
- Global Config
- VLAN Mode

no set igmp querier

Use this command to disable IGMP Snooping Querier on the system. Use the optional *address* parameter to reset the querier address to 0.0.0.0.

Format `no set igmp querier [<vlan-id>] [address]`

Mode
- Global Config
- VLAN Mode

set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default disabled

Format **`set igmp querier query-interval`** *<1-18000>*

Mode Global Config

no set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time to its default value.

Format **`no set igmp querier query-interval`**

Mode Global Config

set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default 60 seconds

Format **`set igmp querier timer expiry`** *<60-300>*

Mode Global Config

no set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period to its default value.

Format **`no set igmp querier timer expiry`**

Mode Global Config

set igmp querier version

Use this command to set the IGMP version of the query that the snooping switch is going to send periodically.

Default 1

Format **`set igmp querier version`** *<1-2>*

Mode Global Config

no set igmp querier version

Use this command to set the IGMP Querier version to its default value.

Format	`no set igmp querier version`
Mode	Global Config

set igmp querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default	disabled
Format	`set igmp querier election participate`
Mode	VLAN Config

no set igmp querier election participate

Use this command to set the Snooping Querier not to participate in querier election but go into non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format	`no set igmp querier election participate`
Mode	VLAN Config

show igmpsnooping querier

Use this command to display IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping Querier is enabled.

Format	`show igmpsnooping querier [{detail | vlan <vlanid>}]`
Mode	Privileged EXEC

When the optional argument <*vlanid*> is not used, the command displays the following information.

Field	*Description*
Admin Mode	Indicates whether or not IGMP Snooping Querier is active on the switch.
Admin Version	The version of IGMP that will be used while sending out the queries.
Querier Address	The IP Address which will be used in the IPv4 header while sending out IGMP queries. It can be configured using the appropriate command.
Query Interval	The amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	The amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for <*vlanid*>, the following additional information appears.

Field	*Description*
VLAN Admin Mode	Indicates whether iGMP Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether IGMP Snooping Querier is in “Querier” or “Non-Querier” state. When the switch is in *Querier* state, it will send out periodic general queries. When in *Non-Querier* state, it will wait for moving to Querier state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participation	Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv4 header while sending out IGMP queries on this VLAN. It can be configured using the appropriate command.
Operational Version	The version of IPv4 will be used while sending out IGMP queries on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument *detail* is used, the command shows the global information and the information for all Querier-enabled VLANs.

PORT SECURITY COMMANDS

This section describes the command you use to configure Port Security on the switch. Port security, which is also known as port MAC locking, allows you to secure the network by locking allowable MAC addresses on a given port. Packets with a matching source MAC address are forwarded normally, and all other packets are discarded.

Note: To enable the SNMP trap specific to port security, see "snmp-server enable traps violation" on page 498.

port-security

This command enables port locking at the system level (Global Config) or port level (Interface Config).

Default disabled

Format `port-security`

Mode
- Global Config
- Interface Config

no port-security

This command disables port locking for one (Interface Config) or all (Global Config) ports.

Format `no port-security`

Mode
- Global Config
- Interface Config

port-security max-dynamic

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port.

Default 600

Format `port-security max-dynamic <maxvalue>`

Mode Interface Config

no port-security max-dynamic

This command resets the maximum number of dynamically locked MAC addresses allowed on a specific port to its default value.

Format `no port-security max-dynamic`

Mode Interface Config

port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a port.

Default	20
Format	**port-security max-static** *<maxvalue>*
Mode	Interface Config

no port-security max-static

This command sets maximum number of statically locked MAC addresses to the default value.

Format	**no port-security max-static**
Mode	Interface Config

port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses. The *<vid>* is the VLAN ID.

Format	**port-security mac-address** *<mac-address> <vid>*
Mode	Interface Config

no port-security mac-address

This command removes a MAC address from the list of statically locked MAC addresses.

Format	**no port-security mac-address** *<mac-address> <vid>*
Mode	Interface Config

port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses.

Format	**port-security mac-address move**
Mode	Interface Config

show port-security

This command displays the port-security settings. If you do not use a parameter, the command displays the settings for the entire system. Use the optional parameters to display the settings on a specific interface or on all interfaces.

Format	**show port-security** *[{<slot/port> | all}]*
Mode	Privileged EXEC

Term	*Definition*
Admin Mode	Port Locking mode for the entire system. This field displays if you do not supply any parameters.

For each interface, or for the interface you specify, the following information appears:

Term	*Definition*
Admin Mode	Port Locking mode for the Interface.
Dynamic Limit	Maximum dynamically allocated MAC Addresses.
Static Limit	Maximum statically allocated MAC Addresses.
Violation Trap Mode	Whether violation traps are enabled.

show port-security dynamic

This command displays the dynamically locked MAC addresses for the port.

Format **show port-security dynamic** *<slot/port>*

Mode Privileged EXEC

Term	*Definition*
MAC Address	MAC Address of dynamically locked MAC.

show port-security static

This command displays the statically locked MAC addresses for port.

Format **show port-security static** *<slot/port>*

Mode Privileged EXEC

Term	*Definition*
MAC Address	MAC Address of statically locked MAC.

show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port.

Format **show port-security violation** *<slot/port>*

Mode Privileged EXEC

Term	*Definition*
MAC Address	MAC Address of discarded packet on locked port.

LLDP (802.1AB) COMMANDS

This section describes the command you use to configure Link Layer Discovery Protocol (LLDP), which is defined in the IEEE 802.1AB specification. LLDP allows stations on an 802 LAN to advertise major capabilities and physical descriptions. The advertisements allow a network management system (NMS) to access and display this information.

lldp transmit

Use this command to enable the LLDP advertise capability.

Default	disabled
Format	`lldp transmit`
Mode	Interface Config

no lldp transmit

Use this command to return the local data transmission capability to the default.

Format	`no lldp transmit`
Mode	Interface Config

lldp receive

Use this command to enable the LLDP receive capability.

Default	disabled
Format	`lldp receive`
Mode	Interface Config

no lldp receive

Use this command to return the reception of LLDPDUs to the default value.

Format	`no lldp receive`
Mode	Interface Config

lldp timers

Use this command to set the timing parameters for local data transmission on ports enabled for LLDP. The *<interval-seconds>* determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 1-32768

seconds. The *<hold-value>* is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2-10. The *<reinit-seconds>* is the delay before re-initialization, and the range is 1-0 seconds.

Default
- interval—30 seconds
- hold—4
- reinit—2 seconds

Format **lldp timers** *[interval <interval-seconds>] [hold <hold-value>] [reinit <reinit-seconds>*]

Mode Global Config

no lldp timers

Use this command to return any or all timing parameters for local data transmission on ports enabled for LLDP to the default values.

Format **no lldp timers** *[interval] [hold] [reinit]*

Mode Global Config

lldp transmit-tlv

Use this command to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs. Use *sys-name* to transmit the system name TLV. To configure the system name, see “snmp-server” on page 496. Use *sys-desc*to transmit the system description TLV. Use *sys-cap* to transmit the system capabilities TLV. Use *port-desc* to transmit the port description TLV. To configure the port description, see See “description” on page 15.

Default no optional TLVs are included

Format **lldp transmit-tlv** *[sys-desc] [sys-name] [sys-cap] [port-desc]*

Mode Interface Config

no lldp transmit-tlv

Use this command to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Format **no lldp transmit-tlv** *[sys-desc] [sys-name] [sys-cap] [port-desc]*

Mode Interface Config

lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs.

Format **lldp transmit-mgmt**

Mode Interface Config

no lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. Use this command to cancel inclusion of the management information in LLDPDUs.

Format	**no lldp transmit-mgmt**
Mode	Interface Config

lldp notification

Use this command to enable remote data change notifications.

Default	disabled
Format	**lldp notification**
Mode	Interface Config

no lldp notification

Use this command to disable notifications.

Default	disabled
Format	**no lldp notification**
Mode	Interface Config

lldp notification-interval

Use this command to configure how frequently the system sends remote data change notifications. The *<interval>* parameter is the number of seconds to wait between sending notifications. The valid interval range is 5-3600 seconds.

Default	5
Format	**lldp notification-interval** *<interval>*
Mode	Global Config

no lldp notification-interval

Use this command to return the notification interval to the default value.

Format	**no lldp notification-interval**
Mode	Global Config

clear lldp statistics

Use this command to reset all LLDP statistics, including MED-related information.

Format	**clear lldp statistics**
Mode	Privileged Exec

clear lldp remote-data

Use this command to delete all information from the LLDP remote data table, including MED-related information.

Format `clear lldp remote-data`

Mode Global Config

show lldp

Use this command to display a summary of the current LLDP configuration.

Format `show lldp`

Mode Privileged Exec

Term	*Definition*
Transmit Interval	How frequently the system transmits local data LLDPDUs, in seconds.
Transmit Hold Multiplier	The multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
Re-initialization Delay	The delay before re-initialization, in seconds.
Notification Interval	How frequently the system sends remote data change notifications, in seconds.

show lldp interface

Use this command to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

Format `show lldp interface` *{<slot/port> | all}*

Mode Privileged Exec

Term	*Definition*
Interface	The interface in a slot/port format.
Link	Shows whether the link is up or down.
Transmit	Shows whether the interface transmits LLDPDUs.
Receive	Shows whether the interface receives LLDPDUs.
Notify	Shows whether the interface sends remote data change notifications.
TLVs	Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Port Description), 1 (System Name), 2 (System Description), or 3 (System Capability).
Mgmt	Shows whether the interface transmits system management address information in the LLDPDUs.

show lldp statistics

Use this command to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Format `show lldp statistics` *{<slot/port> | all}*

Mode Privileged Exec

Term	*Definition*
Last Update	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
Total Inserts	Total number of inserts to the remote data table.
Total Deletes	Total number of deletes from the remote data table.
Total Drops	Total number of times the complete remote data received was not inserted due to insufficient resources.
Total Ageouts	Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

The table contains the following column headings:

Term	*Definition*
Interface	The interface in slot/port format.
Transmit Total	Total number of LLDP packets transmitted on the port.
Receive Total	Total number of LLDP packets received on the port.
Discards	Total number of LLDP frames discarded on the port for any reason.
Errors	The number of invalid LLDP frames received on the port.
Ageouts	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
TVL Discards	The number of TLVs discarded.
TVL Unknowns	Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.

show lldp remote-device

Use this command to display summary information about remote devices that transmit current LLDP data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Format **show lldp remote-device** *{<slot/port> | all}*

Mode Privileged EXEC

Term	*Definition*
Local Interface	The interface that received the LLDPDU from the remote device.
RemID	An internal identifier to the switch to mark each remote device to the system.
Chassis ID	The ID that is sent by a remote device as part of the LLDP message, it is usually a MAC address of the device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show lldp remote-device all

LLDP Remote Device Summary

Local
```



```
Interface RemID    Chassis ID            Port ID             System Name
--------  -------  --------------------  ------------------  ------------------
0/1
0/2
0/3
0/4
0/5
0/6
0/7         2       00:FC:E3:90:01:0F     00:FC:E3:90:01:11
0/7         3       00:FC:E3:90:01:0F     00:FC:E3:90:01:12
0/7         4       00:FC:E3:90:01:0F     00:FC:E3:90:01:13
0/7         5       00:FC:E3:90:01:0F     00:FC:E3:90:01:14
0/7         1       00:FC:E3:90:01:0F     00:FC:E3:90:03:11
0/7         6       00:FC:E3:90:01:0F     00:FC:E3:90:04:11
0/8
0/9
0/10
0/11
0/12
--More-- or (q)uit
```

show lldp remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP data to an interface on the system.

Format **show lldp remote-device detail** *<slot/port>*

Mode Privileged EXEC

Term	*Definition*
Local Interface	The interface that received the LLDPDU from the remote device.
Remote Identifier	An internal identifier to the switch to mark each remote device to the system.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the remote device.
Port ID Subtype	The type of port on the remote device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.
System Description	Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format. The port description is configurable.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.

Term	*Definition*
Time To Live	The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show lldp remote-device detail 0/7

LLDP Remote Device Detail

Local Interface: 0/7


Remote Identifier: 2
Chassis ID Subtype: MAC Address
Chassis ID: 00:FC:E3:90:01:0F
Port ID Subtype: MAC Address
Port ID: 00:FC:E3:90:01:11
System Name:
System Description:
Port Description:
System Capabilities Supported:
System Capabilities Enabled:
Time to Live: 24 seconds
```

show lldp local-device

Use this command to display summary information about the advertised LLDP local data. This command can display summary information or detail for each interface.

Format **show lldp local-device** *{<slot/port> | all}*

Mode Privileged EXEC

Term	*Definition*
Interface	The interface in a slot/port format.
Port ID	The port ID associated with this interface.
Port Description	The port description associated with the interface.

show lldp local-device detail

Use this command to display detailed information about the LLDP data a specific interface transmits.

Format **show lldp local-device detail** *<slot/port>*

Mode Privileged EXEC

Term	*Definition*
Interface	The interface that sends the LLDPDU.
Chassis ID Subtype	The type of identification used in the Chassis ID field.

Term	*Definition*
Chassis ID	The chassis of the local device.
Port ID Subtype	The type of port on the local device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the local device.
System Description	Describes the local system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	The type of address and the specific address the local LLDP agent uses to send and receive information.

LLDP-MED COMMANDS

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) (ANSI-TIA-1057) provides an extension to the LLDP standard. Specifically, LLDP-MED provides extensions for network configuration and policy, device location, Power over Ethernet (PoE) management and inventory management.

lldp med

Use this command to enable MED. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

Default disabled

Format `lldp med`

Mode Interface Config

no lldp med

Use this command to disable MED.

Format `no lldp med`

Mode Interface Config

lldp med confignotification

Use this command to configure all the ports to send the topology change notification.

Default disabled

Format `lldp med confignotification`

Mode Interface Config

no ldp med confignotification

Use this command to disable notifications.

Format `no lldp med confignotification`

Mode Interface Config

lldp med transmit-tlv

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default By default, the capabilities and network policy TLVs are included.

Format `lldp med transmit-tlv` *[capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]*

Mode Interface Config

Term	*Definition*
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format `no lldp med transmit-tlv` *[capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]*

Mode Interface Config

lldp med all

Use this command to configure LLDP-MED on all the ports.

Format `lldp med all`

Mode Global Config

lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Format `lldp med confignotification all`

Mode Global Config

lldp med faststartrepeatcount

Use this command to set the value of the fast start repeat count. *[count]* is the number of LLDP PDUs that will be transmitted when the product is enabled. The range is 1 to 10.

Default 3

Format **lldp med faststartrepeatcount** *[count]*

Mode Global Config

no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Format **no lldp med faststartrepeatcount**

Mode Global Config

lldp med transmit-tlv all

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default By default, the capabilities and network policy TLVs are included.

Format **lldp med transmit-tlv all** *[capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]*

Mode Global Config

Term	*Definition*
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format **no lldp med transmit-tlv** *[capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]*

Mode Global Config

show lldp med

Use this command to display a summary of the current LLDP MED configuration.

Format	**show lldp med**
Mode	Privileged Exec

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show lldp med
LLDP MED Global Configuration

Fast Start Repeat Count:  3
Device Class:  Network Connectivity

(DWS-4026) #
```

show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface. *<slot/port>* indicates a specific physical interface. *all* indicates all valid LLDP interfaces.

Format	**show lldp med interface** *{<slot/port> | all}*
Mode	Privileged Exec

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show lldp med interface all

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
0/1        Down    Disabled  Disabled  Disabled     0,1
0/2        Up      Disabled  Disabled  Disabled     0,1
0/3        Down    Disabled  Disabled  Disabled     0,1
0/4        Down    Disabled  Disabled  Disabled     0,1
0/5        Down    Disabled  Disabled  Disabled     0,1
0/6        Down    Disabled  Disabled  Disabled     0,1
0/7        Down    Disabled  Disabled  Disabled     0,1
0/8        Down    Disabled  Disabled  Disabled     0,1
0/9        Down    Disabled  Disabled  Disabled     0,1
0/10       Down    Disabled  Disabled  Disabled     0,1
0/11       Down    Disabled  Disabled  Disabled     0,1
0/12       Down    Disabled  Disabled  Disabled     0,1
0/13       Down    Disabled  Disabled  Disabled     0,1
0/14       Down    Disabled  Disabled  Disabled     0,1

TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory
--More-- or (q)uit
(DWS-4026) #show lldp med interface 0/2

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
```



```
0/2        Up      Disabled  Disabled  Disabled     0,1

TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory

(DWS-4026) #
```

show lldp med local-device detail

Use this command to display detailed information about the LLDP MED data that a specific interface transmits. *<slot/port> indicates a specific physical interface.*

Format	**show lldp med local-device detail** *<slot/port>*
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show lldp med local-device detail 0/8

LLDP MED Local Device Detail

Interface: 0/8

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True


Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice
```

```
Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
```

show lldp med remote-device

Use this command to display the summary information about remote devices that transmit current LLDP MED data to the system. You can show information about LLDP MED remote data received on all valid LLDP interfaces or on a specific physical interface.

Format **show lldp med remote-device** *{<slot/port> | all}*

Mode Privileged EXEC

Term	*Definition*
Local Interface	The interface that received the LLDPDU from the remote device.
Remote ID	An internal identifier to the switch to mark each remote device to the system.
Device Class	Device classification of the remote device.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show lldp med remote-device all

LLDP MED Remote Device Summary

Local
Interface  Remote ID  Device Class
---------  ---------  ------------
0/8         1         Class I
0/9         2         Not Defined
0/10        3         Class II
0/11        4         Class III
0/12        5         Network Con
```

show lldp med remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP MED data to an interface on the system.

Format **show lldp med remote-device detail** *<slot/port>*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show lldp med remote-device detail 0/8

LLDP MED Remote Device Detail

Local Interface: 0/8
Remote Identifier: 18
Capabilities
MED Capabilities Supported: capabilities, networkpolicy, location, extendedpse
MED Capabilities Enabled: capabilities, networkpolicy
Device Class: Endpoint Class I

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True


Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
```

DENIAL OF SERVICE COMMANDS

This section describes the commands you use to configure Denial of Service (DoS) Control. Unified Switch software provides support for classifying and blocking specific types of Denial of Service attacks. You can configure your system to monitor and block these types of attacks:

- **SIP = DIP:** Source IP address = Destination IP address.
- **First Fragment:**TCP Header size smaller then configured value.
- **TCP Fragment:** IP Fragment Offset = 1.
- **TCP Flag:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port:** Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP:** Limiting the size of ICMP Ping packets.

dos-control all

This command enables Denial of Service protection checks globally.

Default	disabled
Format	`dos-control all`
Mode	Global Config

no dos-control all

This command disables Denial of Service prevention checks globally.

Format	`no dos-control all`
Mode	Global Config

dos-control sipdip

This command enables Source IP address = Destination IP address (SIP = DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP = DIP, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control sipdip`
Mode	Global Config

no dos-control sipdip

This command disables Source IP address = Destination IP address (SIP = DIP) Denial of Service prevention.

Format	`no dos-control sipdip`
Mode	Global Config

dos-control firstfrag

This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller then the configured value, the packets will be dropped if the mode is enabled.The default is *disabled.* If you enable dos-control firstfrag, but do not provide a Minimum TCP Header Size, the system sets that value to *20*.

Default	disabled <20>
Format	**dos-control firstfrag** *[<0-255>]*
Mode	Global Config

no dos-control firstfrag

This command sets Minimum TCP Header Size Denial of Service protection to the default value of *disabled*.

Format	**no dos-control firstfrag**
Mode	Global Config

dos-control tcpfrag

This command enables TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having IP Fragment Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default	disabled
Format	**dos-control tcpfrag**
Mode	Global Config

no dos-control tcpfrag

This command disabled TCP Fragment Denial of Service protection.

Format	**no dos-control tcpfrag**
Mode	Global Config

dos-control tcpflag

This command enables TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attacks. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	**dos-control tcpflag**
Mode	Global Config

no dos-control tcpflag

This command sets disables TCP Flag Denial of Service protections.

Format	`no dos-control tcpflag`
Mode	Global Config

dos-control l4port

This command enables L4 Port Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets will be dropped if the mode is enabled.

Note: Some applications mirror source and destination L4 ports - RIP for example uses 520 for both. If you enable dos-control l4port, applications such as RIP may experience packet loss which would render the application inoperable.

Default	disabled
Format	`dos-control l4port`
Mode	Global Config

no dos-control l4port

This command disables L4 Port Denial of Service protections.

Format	`no dos-control l4port`
Mode	Global Config

dos-control icmp

This command enables Maximum ICMP Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMP Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled <512>
Format	`dos-control icmp` *<0-1023>*
Mode	Global Config

no dos-control icmp

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	`no dos-control icmp`
Mode	Global Config

dos-control smacdmac

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, and BCM56820platforms.

This command enables Source MAC address = Destination MAC address (SMAC = DMAC) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SMAC = DMAC, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control smacdmac`
Mode	Global Config

no dos-control smacdmac

This command disables Source MAC address = Destination MAC address (SMAC = DMAC) Denial of Service protection.

Format	`no dos-control smacdmac`
Mode	Global Config

dos-control tcpport

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, and BCM56820platforms.

This command enables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source TCP Port = Destination TCP Port, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpport`
Mode	Global Config

no dos-control tcpport

This command disables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection.

Format	`no dos-control smacdmac`
Mode	Global Config

dos-control udpport

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, and BCM56820platforms.

This command enables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source UDP Port = Destination UDP Port, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control udpport`
Mode	Global Config

no dos-control udpport

This command disables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection.

Format	`no dos-control udpport`
Mode	Global Config

dos-control tcpflagseq

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, and BCM56820platforms.

This command enables TCP Flag and Sequence Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpflagseq`
Mode	Global Config

no dos-control tcpflagseq

This command sets disables TCP Flag and Sequence Denial of Service protection.

Format	`no dos-control tcpflagseq`
Mode	Global Config

dos-control tcpoffset

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, and BCM56820platforms.

This command enables TCP Offset Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Header Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpoffset`
Mode	Global Config

no dos-control tcpoffset

This command disabled TCP Offset Denial of Service protection.

Format	`no dos-control tcpoffset`
Mode	Global Config

dos-control tcpsyn

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, and BCM56820platforms.

This command enables TCP SYN and L4 source = 0-1023 Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flag SYN set and an L4 source port from 0 to 1023, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpsyn`
Mode	Global Config

no dos-control tcpsyn

This command sets disables TCP SYN and L4 source = 0-1023 Denial of Service protection.

Format	`no dos-control tcpsyn`
Mode	Global Config

dos-control tcpsynfin

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, and BCM56820platforms.

This command enables TCP SYN and FIN Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flags SYN and FIN set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpsynfin`
Mode	Global Config

no dos-control tcpsynfin

This command sets disables TCP SYN & FIN Denial of Service protection.

Format	**no dos-control tcpsynfin**
Mode	Global Config

dos-control tcpfinurgpsh

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, and BCM56820platforms.

This command enables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP FIN, URG, and PSH all set and TCP Sequence Number set to 0, the packets will be dropped if the mode is enabled.

Default	disabled
Format	**dos-control tcpfinurgpsh**
Mode	Global Config

no dos-control tcpfinurgpsh

This command sets disables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections.

Format	**no dos-control tcpfinurgpsh**
Mode	Global Config

dos-control icmpv4

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, and BCM56820platforms.

This command enables Maximum ICMPv4 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv4 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled <512>
Format	**dos-control icmpv4** *<0-16384>*
Mode	Global Config

no dos-control icmpv4

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	**no dos-control icmpv4**
Mode	Global Config

dos-control icmpv6

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, and BCM56820platforms.

This command enables Maximum ICMPv6 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv6 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled <512>
Format	**dos-control icmpv6** *<0-16384>*
Mode	Global Config

no dos-control icmpv6

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	**no dos-control icmpv6**
Mode	Global Config

dos-control icmpfrag

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, and BCM56820platforms.

This command enables ICMP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having fragmented ICMP packets, the packets will be dropped if the mode is enabled.

Default	disabled
Format	**dos-control icmpfrag**
Mode	Global Config

no dos-control icmpfrag

This command disabled ICMP Fragment Denial of Service protection.

Format	**no dos-control icmpfrag**
Mode	Global Config

show dos-control

This command displays Denial of Service configuration information.

Format	**show dos-control**
Mode	Privileged EXEC

Note: Some of the information below displays only if you are using the BCM56224, BCM56514, BCM56624, and BCM56820platforms.

Term	*Definition*
First Fragment Mode	May be enabled or disabled. The factory default is disabled.
Min TCP Hdr Size <0-255>	The factory default is 20.
ICMP Mode	May be enabled or disabled. The factory default is disabled.
Max ICMPv4 Pkt Size	The range is 0-1023. The factory default is 512.
Max ICMPv6 Pkt Size	The range is 0-16384. The factory default is 512.
ICMP Fragment Mode	May be enabled or disabled. The factory default is disabled.
L4 Port Mode	May be enabled or disabled. The factory default is disabled.
TCP Port Mode	May be enabled or disabled. The factory default is disabled.
UDP Port Mode	May be enabled or disabled. The factory default is disabled.
SIPDIP Mode	May be enabled or disabled. The factory default is disabled.
SMACDMAC Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag Mode	May be enabled or disabled. The factory default is disabled.
TCP FIN&URG& PSH Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag & Sequence Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN & FIN Mode	May be enabled or disabled. The factory default is disabled.
TCP Fragment Mode	May be enabled or disabled. The factory default is disabled.
TCP Offset Mode	May be enabled or disabled. The factory default is disabled.

MAC DATABASE COMMANDS

This section describes the commands you use to configure and view information about the MAC databases.

bridge aging-time

This command configures the forwarding database address aging timeout in seconds. The *<seconds>* parameter must be within the range of 10 to 1,000,000 seconds.

Default 300

Format **bridge aging-time** *<10-1,000,000>*

Mode Global Config

no bridge aging-time

This command sets the forwarding database address aging timeout to the default value.

Format **no bridge aging-time**

Mode Global Config

show forwardingdb agetime

This command displays the timeout for address aging. In an IVL system, the [fdbid | all] parameter is required.

Default all

Format **show forwardingdb agetime** *[fdbid | all]*

Mode Privileged EXEC

Term	*Definition*
Forwarding DB ID	Fdbid (Forwarding database ID) indicates the forwarding database whose aging timeout is to be shown. The all option is used to display the aging timeouts associated with all forwarding databases. This field displays the forwarding database ID in an IVL system.
Agetime	• In an IVL system, this parameter displays the address aging timeout for the associated forwarding database. •

show mac-address-table multicast

This command displays the Multicast Forwarding Database (MFDB) information. If you enter the command with no parameter, the entire table is displayed. You can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

Format **show mac-address-table multicast** *<macaddr>*

Mode Privileged EXEC

Term	*Definition*
MAC Address	A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as a MAC address and VLAN ID combination of 8 bytes.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Term	*Definition*
Component	The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, GMRP, and Static Filtering.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
Forwarding Interfaces	The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

show mac-address-table stats

This command displays the Multicast Forwarding Database (MFDB) statistics.

Format `show mac-address-table stats`

Mode Privileged EXEC

Term	*Definition*
Total Entries	The total number of entries that can possibly be in the Multicast Forwarding Database table.
Most MFDB Entries Ever Used	The largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.
Current Entries	The current number of entries in the MFDB.

ISDP COMMANDS

This section describes the commands you use to configure the industry standard Discovery Protocol (ISDP).

isdp run

This command enables ISDP on the switch.

Default Enabled

Format `isdp run`

Mode Global Config

no isdp run

This command disables ISDP on the switch.

Format `no isdp run`

Mode Global Config

isdp holdtime

This command configures the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range is given in seconds.

Default	180 seconds
Format	**isdp holdtime** *<10-255>*
Mode	Global Config

isdp timer

This command sets the period of time between sending new ISDP packets. The range is given in seconds.

Default	30 seconds
Format	**isdp timer** *<5-254>*
Mode	Global Config

isdp advertise-v2

This command enables the sending of ISDP version 2 packets from the device.

Default	Enabled
Format	**isdp advertise-v2**
Mode	Global Config

no isdp advertise-v2

This command disables the sending of ISDP version 2 packets from the device.

Format	**no isdp advertise-v2**
Mode	Global Config

isdp enable

This command enables ISDP on the interface.

Note: ISDP must be enabled both globally and on the interface in order for the interface to transmit ISDP packets. If ISDP is globally disabled on the switch, the interface will not transmit ISDP packets, regardless of the ISDP status on the interface. To enable ISDP globally, use the command “isdp run” on page 156.

Default	Enabled
Format	**isdp enable**
Mode	Interface Config

no isdp enable

This command disables ISDP on the interface.

Format	**no isdp enable**
Mode	Interface Config

clear isdp counters

This command clears ISDP counters.

Format	clear isdp counters
Mode	Privileged EXEC

clear isdp table

This command clears entries in the ISDP table.

Format	**clear isdp table**
Mode	Privileged EXEC

show isdp

This command displays global ISDP settings.

Format	**show isdp**
Mode	Privileged EXEC

Term	*Definition*
Timer	The frequency with which this device sends ISDP packets. This value is given in seconds.
Hold Time	The length of time the receiving device should save information sent by this device. This value is given in seconds.
ISDPv2 Advertisements	The setting for sending ISDPv2 packets. If disabled, version 1 packets are transmitted.
Device ID	The Device ID advertised by this device. The format of this Device ID is characterized by the value of the Device ID Format object.
Device ID Format Capability	Indicates the Device ID format capability of the device. • serialNumber indicates that the device uses a serial number as the format for its Device ID. • macAddress indicates that the device uses a Layer 2 MAC address as the format for its Device ID. • other indicates that the device uses its platform-specific format as the format for its Device ID.
Device ID Format	Indicates the Device ID format of the device. • serialNumber indicates that the value is in the form of an ASCII string containing the device serial number. • macAddress indicates that the value is in the form of a Layer 2 MAC address. • other indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example, ASCII string contains serialNumber appended/prepended with system name.

show isdp interface

This command displays ISDP settings for the specified interface.

Format **show isdp interface** *{all | <slot/port>}*

Mode Privileged EXEC

Term	*Definition*
Mode	ISDP mode enabled/disabled status for the interface(s).

show isdp entry

This command displays ISDP entries. If the device id is specified, then only entries for that device are shown.

Format **show isdp entry** *{all | deviceid}*

Mode Privileged EXEC

Term	*Definition*
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP address(es) associated with the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Version	The software version that the neighbor is running.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Capability	ISDP Functional Capabilities advertised by the neighbor.

show isdp neighbors

This command displays the list of neighboring devices.

Format **show isdp neighbors** *[{<slot/port> | detail}]*

Mode Privileged EXEC

Term	*Definition*
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP addresses associated with the neighbor.
Capability	ISDP functional capabilities advertised by the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Entry Last Changed Time	Displays when the entry was last modified.
Version	The software version that the neighbor is running.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show isdp neighbors detail

Device ID                  0001f45f1bc0
Address(es):
    IP Address:            10.27.7.57
Capability                 Router Trans Bridge Switch IGMP
Platform                   SecureStack C2
Interface                  0/48
Port ID                    ge.3.14
Holdtime                   131
Advertisement Version      2
Entry last changed time    0 days 00:01:59
Version:                   05.00.56
```

show isdp traffic

This command displays ISDP statistics.

Format show isdp traffic

Mode Privileged EXEC

Term	*Definition*
ISDP Packets Received	Total number of ISDP packets received
ISDP Packets Transmitted	Total number of ISDP packets transmitted

Term	*Definition*
ISDPv1 Packets Received	Total number of ISDPv1 packets received
ISDPv1 Packets Transmitted	Total number of ISDPv1 packets transmitted
ISDPv2 Packets Received	Total number of ISDPv2 packets received
ISDPv2 Packets Transmitted	Total number of ISDPv2 packets transmitted
ISDP Bad Header	Number of packets received with a bad header
ISDP Checksum Error	Number of packets received with a checksum error
ISDP Transmission Failure	Number of packets which failed to transmit
ISDP Invalid Format	Number of invalid packets received
ISDP Table Full	Number of times a neighbor entry was not added to the table due to a full database
ISDP IP Address Table Full	Displays the number of times a neighbor entry was added to the table without an IP address.

debug isdp packet

This command enables tracing of ISDP packets processed by the switch. ISDP must be enabled on both the device and the interface in order to monitor packets for a particular interface.

Format `debug isdp packet` *`[{receive | transmit}]`*

Mode Privileged EXEC

no debug isdp packet

This command disables tracing of ISDP packets on the receive or the transmit sides or on both sides.

Format `no debug isdp packet` *`[{receive | transmit}]`*

Mode Privileged EXEC

Section 4: Routing Commands

This section describes the routing commands available in the Unified Switch CLI.

The Routing Commands section contains the following subsections:

Note: The commands in this section are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

Address Resolution Protocol Commands

This section describes the commands you use to configure Address Resolution Protocol (ARP) and to view ARP information on the switch. ARP associates IP addresses with MAC addresses and stores the information as ARP entries in the ARP cache.

arp

This command creates an ARP entry. The value for *<ipaddress>* is the IP address of a device on a subnet attached to an existing routing interface. *<macaddr>* is a unicast MAC address for that device.

The format of the MAC address is 6 two-digit hexadecimal numbers that are separated by colons, for example 00:06:29:32:81:40.

Format	**arp** *<ipaddress> <macaddr>*
Mode	Global Config

no arp

This command deletes an ARP entry. The value for *<arpentry>* is the IP address of the interface. The value for *<ipaddress>* is the IP address of a device on a subnet attached to an existing routing interface. *<macaddr>* is a unicast MAC address for that device.

Format	**no arp** *<ipaddress> <macaddr>*
Mode	Global Config

ip proxy-arp

This command enables proxy ARP on a router interface. Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request.

Default	enabled
Format	**ip proxy-arp**
Mode	Interface Config

no ip proxy-arp

This command disables proxy ARP on a router interface.

Format	**no ip proxy-arp**
Mode	Interface Config

arp cachesize

This command configures the ARP cache size. The ARP cache size value is a platform specific integer value. The default size also varies depending on the platform.

Format	**arp cachesize** *<platform specific integer value>*
Mode	Global Config

no arp cachesize

This command configures the default ARP cache size.

Format	**no arp cachesize**
Mode	Global Config

arp dynamicrenew

This command enables the ARP component to automatically renew dynamic ARP entries when they age out.

Default	disabled
Format	**arp dynamicrenew**
Mode	Privileged EXEC

no arp dynamicrenew

This command prevents dynamic ARP entries from renewing when they age out.

Format	**no arp dynamicrenew**
Mode	Privileged EXEC

arp purge

This command causes the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

Format	**arp purge** *<ipaddr>*
Mode	Privileged EXEC

arp resptime

This command configures the ARP request response timeout.

The value for *<seconds>* is a valid positive integer, which represents the IP ARP entry response timeout time in seconds. The range for *<seconds>* is between 1-10 seconds.

Default	1
Format	**arp resptime** *<1-10>*
Mode	Global Config

no arp resptime

This command configures the default ARP request response timeout.

Format	**no arp resptime**
Mode	Global Config

arp retries

This command configures the ARP count of maximum request for retries.

The value for *<retries>* is an integer, which represents the maximum number of request for retries. The range for *<retries>* is an integer between 0-10 retries.

Default	4
Format	**arp retries** *<0-10>*
Mode	Global Config

no arp retries

This command configures the default ARP count of maximum request for retries.

Format	**no arp retries**
Mode	Global Config

arp timeout

This command configures the ARP entry ageout time.

The value for *<seconds>* is a valid positive integer, which represents the IP ARP entry ageout time in seconds. The range for *<seconds>* is between 15-21600 seconds.

Default	1200
Format	**arp timeout** *<15-21600>*
Mode	Global Config

no arp timeout

This command configures the default ARP entry ageout time.

Format	**no arp timeout**
Mode	Global Config

clear arp-cache

This command causes all ARP entries of type dynamic to be removed from the ARP cache. If the *gateway* keyword is specified, the dynamic entries of type gateway are purged as well.

Format	**clear arp-cache** *[gateway]*
Mode	Privileged EXEC

clear arp-switch

Use this command to clear the contents of the switch's Address Resolution Protocol (ARP) table that contains entries learned through the Management port. To observe whether this command is successful, **ping** from the remote system to the DUT. Issue the **show arp switch** command to see the ARP entries. Then issue the **clear arp-switch** command and check the **show arp switch** entries. There will be no more arp entries.

Format	**clear arp-switch**
Mode	Privileged EXEC

show arp

This command displays the Address Resolution Protocol (ARP) cache. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the **`show arp`** results in conjunction with the **`show arp switch`** results.

Format **`show arp`**

Mode Privileged EXEC

Term	*Definition*
Age Time (seconds)	The time it takes for an ARP entry to age out. This is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

The following are displayed for each ARP entry:

Term	*Definition*
IP Address	The IP address of a device on a subnet attached to an existing routing interface.
MAC Address	The hardware MAC address of that device.
Interface	The routing slot/port associated with the device ARP entry.
Type	The type that is configurable. The possible values are Local, Gateway, Dynamic and Static.
Age	The current age of the ARP entry since last refresh (in hh:mm:ss format)

show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information.

Format **`show arp brief`**

Mode Privileged EXEC

Term	*Definition*
Age Time (seconds)	The time it takes for an ARP entry to age out. This value is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.

Term	*Definition*
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

show arp switch

This command displays the contents of the switch's Address Resolution Protocol (ARP) table.

Format `show arp switch`

Mode Privileged EXEC

Term	*Definition*
IP Address	The IP address of a device on a subnet attached to the switch.
MAC Address	The hardware MAC address of that device.
Interface	The routing slot/port associated with the device's ARP entry.

IP ROUTING COMMANDS

This section describes the commands you use to enable and configure IP routing on the switch.

routing

This command enables routing for an interface. You can view the current value for this function with the **`show ip brief`** command. The value is labeled as "Routing Mode."

Default disabled

Format `routing`

Mode Interface Config

no routing

This command disables routing for an interface.

You can view the current value for this function with the **`show ip brief`** command. The value is labeled as "Routing Mode."

Format `no routing`

Mode Interface Config

ip routing

This command enables the IP Router Admin Mode for the master switch.

Format	**ip routing**
Mode	Global Config

no ip routing

This command disables the IP Router Admin Mode for the master switch.

Format	**no ip routing**
Mode	Global Config

ip address

This command configures an IP address on an interface. You can also use this command to configure one or more secondary IP addresses on the interface.The value for *<ipaddr>* is the IP address of the interface. The value for *<subnetmask>* is a 4-digit dotted-decimal number which represents the subnet mask of the interface. The subnet mask must have contiguous ones and be no longer than 30 bits, for example 255.255.255.0. This command adds the label IP address in **show ip interface**.

Format	**ip address** *<ipaddr> <subnetmask> [secondary]*
Mode	Interface Config

no ip address

This command deletes an IP address from an interface. The value for *<ipaddr>* is the IP address of the interface in a.b.c.d format where the range for a, b, c, and d is 1-255. The value for *<subnetmask>* is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface. To remove all of the IP addresses (primary and secondary) configured on the interface, enter the command **no ip address**.

Format	**no ip address** *[{<ipaddr> <subnetmask> [secondary]}]*
Mode	Interface Config

ip route

This command configures a static route. The *<ipaddr>* parameter is a valid IP address, and *<subnetmask>* is a valid subnet mask. The *<nexthopip>* parameter is a valid IP address of the next hop router. Specifying `Null0` as nexthop parameter adds a static reject route. The optional *<preference>* parameter is an integer (value from 1 to 255) that allows you to specify the preference value (sometimes called “administrative distance”) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination. A route with a preference of 255 cannot be used to forward traffic.

For the static routes to be visible, you must perform the following steps:

- Enable ip routing globally.
- Enable ip routing for the interface.
- Confirm that the associated link is also up.

Default	preference—1
Format	**ip route** *<ipaddr> <subnetmask> [<nexthopip> | Null0] [<preference>]*
Mode	Global Config

no ip route

This command deletes a single next hop to a destination static route. If you use the *<nexthopip>* parameter, the next hop is deleted. If you use the *<preference>* value, the preference value of the static route is reset to its default.

Format	**no ip route** *<ipaddr> <subnetmask> [{<nexthopip> [<preference>] | Null0}]*
Mode	Global Config

ip route default

This command configures the default route. The value for *<nexthopip>* is a valid IP address of the next hop router. The *<preference>* is an integer value from 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

Default	preference—1
Format	**ip route default** *<nexthopip> [<preference>]*
Mode	Global Config

no ip route default

This command deletes all configured default routes. If the optional *<nexthopip>* parameter is designated, the specific next hop is deleted from the configured default route and if the optional preference value is designated, the preference of the configured default route is reset to its default.

Format	**no ip route default** *[{<nexthopip> | <preference>}]*
Mode	Global Config

ip route distance

This command sets the default distance (preference) for static routes. Lower route distance values are preferred when determining the best route. The **ip route** and **ip route default** commands allow you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the **ip route distance** command.

Default	1
Format	**ip route distance** *<1-255>*
Mode	Global Config

no ip route distance

This command sets the default static route preference value in the router. Lower route preference values are preferred when determining the best route.

Format	`no ip route distance`
Mode	Global Config

ip netdirbcast

This command enables the forwarding of network-directed broadcasts. When enabled, network directed broadcasts are forwarded. When disabled they are dropped.

Default	disabled
Format	`ip netdirbcast`
Mode	Interface Config

no ip netdirbcast

This command disables the forwarding of network-directed broadcasts. When disabled, network directed broadcasts are dropped.

Format	`no ip netdirbcast`
Mode	Interface Config

ip mtu

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Unified Switch software currently does not fragment IP packets.

- Packets forwarded in hardware ignore the IP MTU.
- Packets forwarded in software are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, may be fragmented by the IP stack. The IP stack uses its default IP MTU and ignores the value set using the ip mtu command.

Note: The IP MTU size refers to the maximum size of the IP packet (IP Header + IP payload). It does not include any extra bytes that may be required for Layer-2 headers. To receive and process packets, the Ethernet MTU (see “mtu” on page 15) must take into account the size of the Ethernet header.

Default	1500 bytes
Format	`ip mtu` *<68-1500>*
Mode	Interface Config

no ip mtu

This command resets the ip mtu to the default value.

Format	**no ip mtu** *<mtu>*
Mode	Interface Config

encapsulation

This command configures the link layer encapsulation type for the packet. The encapsulation type can be *ethernet* or *snap*.

Default	ethernet
Format	**encapsulation** *{ethernet | snap}*
Mode	Interface Config

Note: Routed frames are always ethernet encapsulated when a frame is routed to a VLAN.

show ip brief

This command displays all the summary information of the IP, including the ICMP rate limit configuration and the global ICMP Redirect configuration.

Format	**show ip brief**
Modes	• Privileged EXEC • User EXEC

Term	*Definition*
Default Time to Live	The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.
Routing Mode	Shows whether the routing mode is enabled or disabled.
Maximum Next Hops	The maximum number of next hops the packet can travel.
Maximum Routes	The maximum number of routes the packet can travel.
ICMP Rate Limit Interval	Shows how often the token bucket is initialized with burst-size tokens. *Burst-interval* is from 0 to 2147483647 milliseconds. The default *burst-interval* is 1000 msec.
ICMP Rate Limit Burst Size	Shows the number of ICMPv4 error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages. The default value is 100 messages.
ICMP Echo Replies	Shows whether ICMP Echo Replies are enabled or disabled.
ICMP Redirects	Shows whether ICMP Redirects are enabled or disabled.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show ip brief

Default Time to Live.......................... 64
Routing Mode.................................. Disabled
Maximum Next Hops............................. 4
```



```
Maximum Routes.............................. 6000
ICMP Rate Limit Interval.................... 1000 msec
ICMP Rate Limit Burst Size.................. 100 messages
ICMP Echo Replies........................... Enabled
ICMP Redirects.............................. Enabled
```

show ip interface

This command displays all pertinent information about the IP interface.

Format **show ip interface** *<slot/port>*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Routing Interface Status	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
Primary IP Address	The primary IP address and subnet masks for the interface. This value appears only if you configure it.
Secondary IP Address	One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.
Helper IP Address	The helper IP addresses configured by the "ip helper-address" command.
Routing Mode	The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.
Administrative Mode	The administrative mode of the specified interface. The possible values of this field are enable or disable. This value is configurable.
Forward Net Directed Broadcasts	Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value is configurable.
Proxy ARP	Displays whether Proxy ARP is enabled or disabled on the system.
Local Proxy ARP	Displays whether Local Proxy ARP is enabled or disabled on the interface.
Active State	Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.
Link Speed Data Rate	An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
MAC Address	The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
Encapsulation Type	The encapsulation type for the specified interface. The types are: Ethernet or SNAP.
IP MTU	The maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth	Shows the bandwidth of the interface.
Destination Unreachables	Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).
ICMP Redirects	Displays whether ICMP Redirects may be sent (enabled or disabled).

Example: The following shows example CLI display output for the command.

```
(DWS-4026)#show ip interface 0/2

Routing Interface Status..................... Down
```

```
   Primary IP Address.............................. 1.2.3.4/255.255.255.0
   Secondary IP Address(es)........................ 21.2.3.4/255.255.255.0
   ................................................ 22.2.3.4/255.255.255.0
   Helper IP Address............................... 1.2.3.4
   ................................................ 1.2.3.5
   Routing Mode.................................... Disable
Administrative Mode............................... Enable
Forward Net Directed Broadcasts................... Disable
Proxy ARP......................................... Enable
Local Proxy ARP................................... Disable
Active State...................................... Inactive
Link Speed Data Rate.............................. Inactive
MAC Address....................................... 00:10:18:82:0C:68
Encapsulation Type................................ Ethernet
IP MTU............................................ 1500
Bandwidth......................................... 100000 kbps
Destination Unreachables.......................... Enabled
ICMP Redirects.................................... Enabled
```

show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router.

Format `show ip interface brief`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
State	Routing operational state of the interface.
IP Address	The IP address of the routing interface in 32-bit dotted decimal format.
IP Mask	The IP mask of the routing interface in 32-bit dotted decimal format.
Netdir Bcast	Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.
MultiCast Fwd	The multicast forwarding administrative mode on the interface. Possible values are Enable or Disable.

show ip route

This command displays the routing table. The *<ip-address>* specifies the network for which the route is to be displayed and displays the best matching best-route for the address. The *<mask>* specifies the subnet mask for the given *<ip-address>*. When you use the *longer-prefixes* keyword, the *<ip-address>* and *<mask>* pair becomes the prefix, and the command displays the routes to the addresses that match that prefix. Use the *<protocol>* parameter to specify the protocol that installed the routes. The value for *<protocol>* can be *connected*, *rip*, or *static*. Use the *all* parameter to display all routes including best and non-best routes. If you do not use the *all* parameter, the command only displays the best route.

Note: If you use the *connected* keyword for *<protocol>*, the *all* option is not available because there are no best or non-best connected routes.

Format **show ip route** *[{<ip-address> [<protocol>] | {<ip-address> <mask> [longer-prefixes] [<protocol>] | <protocol>} [all] | all}]*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Route Codes	The key for the routing protocol codes that might appear in the routing table output.

The **show ip route** command displays the routing tables in the following format:

```
Code   IP-Address/Mask [Preference/Metric] via Next-Hop, Route-Timestamp, Interface
```

The columns for the routing table display the following information:

Term	*Definition*
Code	The codes for the routing protocols that created the routes.
IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Route-Timestamp	The last updated time for dynamic routes. The format of Route-Timestamp will be • Days:Hours:Minutes if days > = 1 • Hours:Minutes:Seconds if days < 1
Interface	The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be Null0 interface.

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the router, you can configure a static reject route on the router. Such traffic would be discarded and the ICMP destination unreachable message is sent back to the source. This is typically used for preventing routing loops. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by RIP.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show ip route

Route Codes: R - RIP Derived, C - Connected, S - Static

C 1.1.1.0/24 [0/1] directly connected, 0/11
C 2.2.2.0/24 [0/1] directly connected, 0/1
C 5.5.5.0/24 [0/1] directly connected, 0/5
S 7.0.0.0/8 [1/0] directly connected, Null0
OIA 10.10.10.0/24 [110/6] via 5.5.5.2,   00h:00m:01s,  0/5
C 11.11.11.0/24 [0/1] directly connected,   0/11
S 12.0.0.0/8 [5/0] directly connected, Null0
S 23.0.0.0/8 [3/0] directly connected, Null0
```

show ip route summary

Use this command to display the routing table summary. Use the optional *all* parameter to show the number of all routes, including best and non-best routes. To include only the number of best routes, do not use the optional parameter.

Format **show ip route summary** *[all]*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Connected Routes	The total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
RIP Routes	Total number of routes installed by RIP protocol.
Reject Routes	Total number of reject routes installed by all protocols.
Total Routes	Total number of routes in the routing table.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show ip route summary

Connected Routes.............................1
Static Routes................................7
RIP Routes...................................0
Reject Routes................................2
Total routes.................................8
```

show ip route preferences

This command displays detailed information about the route preferences. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values. A route with a preference of 255 cannot be used to forward traffic.

Format **show ip route preferences**

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Local	The local route preference value.
Static	The static route preference value.
RIP	The RIP route preference value.

show ip stats

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Format `show ip stats`

Modes
- Privileged EXEC
- User EXEC

ROUTER DISCOVERY PROTOCOL COMMANDS

This section describes the commands you use to view and configure Router Discovery Protocol settings on the switch. The Router Discovery Protocol enables a host to discover the IP address of routers on the subnet.

ip irdp

This command enables Router Discovery on an interface.

Default disabled

Format `ip irdp`

Mode Interface Config

no ip irdp

This command disables Router Discovery on an interface.

Format `no ip irdp`

Mode Interface Config

ip irdp address

This command configures the address that the interface uses to send the router discovery advertisements. The valid values for *<ipaddr>* are 224.0.0.1, which is the all-hosts IP multicast address, and 255.255.255.255, which is the limited broadcast address.

Default 224.0.0.1

Format `ip irdp address` *<ipaddr>*

Mode Interface Config

no ip irdp address

This command configures the default address used to advertise the router for the interface.

Format `no ip irdp address`

Mode Interface Config

ip irdp holdtime

This command configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface. The holdtime range is the value of *<maxadvertinterval>* to 9000 seconds.

Default	3 * maxinterval
Format	**ip irdp holdtime** *<maxadvertinterval-9000>*
Mode	Interface Config

no ip irdp holdtime

This command configures the default value, in seconds, of the holdtime field of the router advertisement sent from this interface.

Format	**no ip irdp holdtime**
Mode	Interface Config

ip irdp maxadvertinterval

This command configures the maximum time, in seconds, allowed between sending router advertisements from the interface. The range for maxadvertinterval is 4 to 1800 seconds.

Default	600
Format	**ip irdp maxadvertinterval** *<4-1800>*
Mode	Interface Config

no ip irdp maxadvertinterval

This command configures the default maximum time, in seconds.

Format	**no ip irdp maxadvertinterval**
Mode	Interface Config

ip irdp minadvertinterval

This command configures the minimum time, in seconds, allowed between sending router advertisements from the interface. The range for minadvertinterval is three to the value of maxadvertinterval.

Default	0.75 * maxadvertinterval
Format	**ip irdp minadvertinterval** *<3-maxadvertinterval>*
Mode	Interface Config

no ip irdp minadvertinterval

This command sets the default minimum time to the default.

Format	**no ip irdp minadvertinterval**
Mode	Interface Config

ip irdp preference

This command configures the preferability of the address as a default router address, relative to other router addresses on the same subnet.

Default 0

Format **ip irdp preference** *<-2147483648 to 2147483647>*

Mode Interface Config

no ip irdp preference

This command configures the default preferability of the address as a default router address, relative to other router addresses on the same subnet.

Format **no ip irdp preference**

Mode Interface Config

show ip irdp

This command displays the router discovery information for all interfaces, or a specified interface.

Format **show ip irdp** *{<slot/port> | all}*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	The *<slot/port>* that matches the rest of the information in the row.
Ad Mode	The advertise mode, which indicates whether router discovery is enabled or disabled on this interface.
Advertise Address	The IP address to which the interface sends the advertisement.
Max Int	The maximum advertise interval, which is the maximum time, in seconds, allowed between sending router advertisements from the interface.
Min Int	The minimum advertise interval, which is the minimum time, in seconds, allowed between sending router advertisements from the interface.
Hold Time	The amount of time, in seconds, that a system should keep the router advertisement before discarding it.
Preference	The preference of the address as a default router address, relative to other router addresses on the same subnet.

VIRTUAL LAN ROUTING COMMANDS

This section describes the commands you use to view and configure VLAN routing and to view VLAN routing status information.

vlan routing

This command creates routing on a VLAN. The *<vlanid>* value has a range from 1 to 3965.

Format **vlan routing** *<vlanid>*

Mode VLAN Config

no vlan routing

This command deletes routing on a VLAN. The *<vlanid>* value has a range from 1 to 3965.

Format **no vlan routing** *<vlanid>*

Mode VLAN Config

show ip vlan

This command displays the VLAN routing information for all VLANs with routing enabled.

Format **show ip vlan**

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
MAC Address used by Routing VLANs	The MAC Address associated with the internal bridge-router interface (IBRI). The same MAC Address is used by all VLAN routing interfaces. It will be displayed above the per-VLAN information.
VLAN ID	The identifier of the VLAN.
Logical Interface	The logical slot/port associated with the VLAN routing interface.
IP Address	The IP address associated with this VLAN.
Subnet Mask	The subnet mask that is associated with this VLAN.

VIRTUAL ROUTER REDUNDANCY PROTOCOL COMMANDS

This section describes the commands you use to view and configure Virtual Router Redundancy Protocol (VRRP) and to view VRRP status information. VRRP helps provide failover and load balancing when you configure two devices as a VRRP pair.

ip vrrp (Global Config)

Use this command in Global Config mode to enable the administrative mode of VRRP on the router.

Default none

Format **ip vrrp**

Mode Global Config

no ip vrrp

Use this command in Global Config mode to disable the default administrative mode of VRRP on the router.

Format **no ip vrrp**

Mode Global Config

ip vrrp (Interface Config)

Use this command in Interface Config mode to create a virtual router associated with the interface. The parameter *<vrid>* is the virtual router ID, which has an integer value range from 1 to 255.

Format **ip vrrp** *<vrid>*

Mode Interface Config

no ip vrrp

Use this command in Interface Config mode to delete the virtual router associated with the interface. The virtual Router ID, *<vrid>*, is an integer value that ranges from 1 to 255.

Format **no ip vrrp** *<vrid>*

Mode Interface Config

ip vrrp mode

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router. The parameter *<vrid>* is the virtual router ID which has an integer value ranging from 1 to 255.

Default disabled

Format **ip vrrp** *<vrid>* **mode**

Mode Interface Config

no ip vrrp mode

This command disables the virtual router configured on the specified interface. Disabling the status field stops a virtual router.

Format **no ip vrrp** *<vrid>* **mode**

Mode Interface Config

ip vrrp ip

This command sets the virtual router IP address value for an interface. The value for *<ipaddr>* is the IP address which is to be configured on that interface for VRRP. The parameter *<vrid>* is the virtual router ID which has an integer value range from 1 to 255. You can use the optional *[secondary]* parameter to designate the IP address as a secondary IP address.

Default none

Format **ip vrrp** *<vrid>* **ip** *<ipaddr> [secondary]*

Mode Interface Config

no ip vrrp ip

Use this command in Interface Config mode to delete a secondary IP address value from the interface. To delete the primary IP address, you must delete the virtual router on the interface.

Format **no ip vrrp** *<vrid> <ipaddress> secondary*

Mode Interface Config

ip vrrp authentication

This command sets the authorization details value for the virtual router configured on a specified interface. The parameter *{none | simple}* specifies the authorization type for virtual router configured on the specified interface. The parameter *[key]* is optional, it is only required when authorization type is simple text password. The parameter *<vrid>* is the virtual router ID which has an integer value ranges from 1 to 255.

Default no authorization

Format **ip vrrp** *<vrid>* **authentication** *{none | simple <key>}*

Mode Interface Config

no ip vrrp authentication

This command sets the default authorization details value for the virtual router configured on a specified interface.

Format **no ip vrrp** *<vrid>* **authentication**

Mode Interface Config

ip vrrp preempt

This command sets the preemption mode value for the virtual router configured on a specified interface. The parameter *<vrid>* is the virtual router ID, which is an integer from 1 to 255.

Default	enabled
Format	**ip vrrp** *<vrid>* **preempt**
Mode	Interface Config

no ip vrrp preempt

This command sets the default preemption mode value for the virtual router configured on a specified interface.

Format	**no ip vrrp** *<vrid>* **preempt**
Mode	Interface Config

ip vrrp priority

This command sets the priority of a router within a VRRP group. Higher values equal higher priority. The range is from 1 to 254. The parameter *<vrid>* is the virtual router ID, whose range is from 1 to 255.

The router with the highest priority is elected master. If a router is configured with the address used as the address of the virtual router, the router is called the “address owner.” The priority of the address owner is always 255 so that the address owner is always master. If the master has a priority less than 255 (it is not the address owner) and you configure the priority of another router in the group higher than the master’s priority, the router will take over as master only if preempt mode is enabled.

Default	100 unless the router is the address owner, in which case its priority is automatically set to 255.
Format	**ip vrrp** *<vrid>* **priority** *<1-254>*
Mode	Interface Config

no ip vrrp priority

This command sets the default priority value for the virtual router configured on a specified interface.

Format	**no ip vrrp** *<vrid>* **priority**
Mode	Interface Config

ip vrrp timers advertise

This command sets the frequency, in seconds, that an interface on the specified virtual router sends a virtual router advertisement.

Default	1
Format	**ip vrrp** *<vrid>* **timers advertise** *<1-255>*
Mode	Interface Config

no ip vrrp timers advertise

This command sets the default virtual router advertisement value for an interface.

Format	**no ip vrrp** *<vrid>* **timers advertise**
Mode	Interface Config

ip vrrp track interface

Use this command to alter the priority of the VRRP router based on the availability of its interfaces. This command is useful for tracking interfaces that are not configured for VRRP. Only IP interfaces are tracked. A tracked interface is up if the IP on that interface is up. Otherwise, the tracked interface is down.

When the tracked interface is down or the interface has been removed from the router, the priority of the VRRP router will be decremented by the value specified in the *<priority>* argument. When the interface is up for IP protocol, the priority will be incremented by the *<priority>* value.

A VRRP configured interface can track more than one interface. When a tracked interface goes down, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed interface. The default priority decrement is changed using the *<priority>* argument. The default priority of the virtual router is 100, and the default decrement priority is 10. By default, no interfaces are tracked. If you specify just the interface to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10.

Default	priority: 10
Format	**ip vrrp** *<vrid>* **track interface** *<slot/port> [decrement <priority>]*
Mode	Interface Config

no ip vrrp track interface

Use this command to remove the interface from the tracked list or to restore the priority decrement to its default.

Format	**no ip vrrp** *<vrid>* **track interface** *<slot/port> [decrement]*
Mode	Interface Config

ip vrrp track ip route

Use this command to track the route reachability. When the tracked route is deleted, the priority of the VRRP router will be decremented by the value specified in the *<priority>* argument. When the tracked route is added, the priority will be incremented by the same.

A VRRP configured interface can track more than one route. When a tracked route goes down, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed route. By default no routes are tracked. If you specify just the route to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10. The default priority decrement is changed using the *<priority>* argument.

Default	priority: 10
Format	**ip vrrp** *<vrid>* **track ip route** *<ip-address/prefix-length> [decrement <priority>]*
Mode	Interface Config

no ip vrrp track ip route

Use this command to remove the route from the tracked list or to restore the priority decrement to its default. When removing a tracked IP route from the tracked list, the priority should be incremented by the decrement value if the route is not reachable.

Format **no ip vrrp** *<vrid>* **track interface** *<slot/port> [decrement]*

Mode Interface Config

show ip vrrp interface stats

This command displays the statistical information about each virtual router configured on the switch.

Format **show ip vrrp interface stats** *<slot/port> <vrid>*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Uptime	The time that the virtual router has been up, in days, hours, minutes and seconds.
Protocol	The protocol configured on the interface.
State Transitioned to Master	The total number of times virtual router state has changed to MASTER.
Advertisement Received	The total number of VRRP advertisements received by this virtual router.
Advertisement Interval Errors	The total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.
Authentication Failure	The total number of VRRP packets received that don't pass the authentication check.
IP TTL errors	The total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.
Zero Priority Packets Received	The total number of VRRP packets received by virtual router with a priority of '0'.
Zero Priority Packets Sent	The total number of VRRP packets sent by the virtual router with a priority of '0'.
Invalid Type Packets Received	The total number of VRRP packets received by the virtual router with invalid 'type' field.
Address List Errors	The total number of VRRP packets received for which address list does not match the locally configured list for the virtual router.
Invalid Authentication Type	The total number of VRRP packets received with unknown authentication type.
Authentication Type Mismatch	The total number of VRRP advertisements received for which 'auth type' not equal to locally configured one for this virtual router.
Packet Length Errors	The total number of VRRP packets received with packet length less than length of VRRP header.

show ip vrrp

This command displays whether VRRP functionality is enabled or disabled on the switch. It also displays some global parameters which are required for monitoring. This command takes no options.

Format `show ip vrrp`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
VRRP Admin Mode	The administrative mode for VRRP functionality on the switch.
Router Checksum Errors	The total number of VRRP packets received with an invalid VRRP checksum value.
Router Version Errors	The total number of VRRP packets received with Unknown or unsupported version number.
Router VRID Errors	The total number of VRRP packets received with invalid VRID for this virtual router.

show ip vrrp interface

This command displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface. Use the output of the command to verify the track interface and track IP route configurations.

Format **`show ip vrrp interface`** *<slot/port> <vrid>*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
IP Address	The configured IP address for the Virtual router.
VMAC address	The VMAC address of the specified router.
Authentication type	The authentication type for the specific virtual router.
Priority	The priority value for the specific virtual router, taking into account any priority decrements for tracked interfaces or routes.
Configured Priority	The priority configured through the **`ip vrrp`** *<vrid>* **`priority`** *<1-254>* command.
Advertisement interval	The advertisement interval in seconds for the specific virtual router.
Pre-Empt Mode	The preemption mode configured on the specified virtual router.
Administrative Mode	The status (Enable or Disable) of the specific router.
State	The state (Master/backup) of the virtual router.

Example: The following shows example CLI display output for the command.

```
show ip vrrp interface <u/s/p> <vrid>

Primary IP Address.............................. 1.1.1.5
VMAC Address.................................... 00:00:5e:00:01:01
```



```
Authentication Type.......................... None
Priority..................................... 80
  Configured priority........................ 100
Advertisement Interval (secs)................ 1
Pre-empt Mode................................ Enable
Administrative Mode.......................... Enable
State........................................ Initialized

Track Interface          State          DecrementPriority
---------------         ------          -----------------

<0/1>                  down                10

TrackRoute  (pfx/len)   State        DecrementPriority
-----------------------   ------         -----------------
10.10.10.1/255.255.255.0    down              10
```

show ip vrrp interface brief

This command displays information about each virtual router configured on the switch. This command takes no options. It displays information about each virtual router.

Format **`show ip vrrp interface brief`**

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
VRID	The router ID of the virtual router.
IP Address	The virtual router IP address.
Mode	Indicates whether the virtual router is enabled or disabled.
State	The state (Master/backup) of the virtual router.

DHCP AND BOOTP RELAY COMMANDS

This section describes the commands you use to configure BootP/DHCP Relay on the switch. A DHCP relay agent operates at Layer 3 and forwards DHCP requests and replies between clients and servers when they are not on the same physical subnet.

bootpdhcprelay cidoptmode

This command enables the circuit ID option mode for BootP/DHCP Relay on the system.

Default disabled

Format **`bootpdhcprelay cidoptmode`**

Mode Global Config

no bootpdhcprelay cidoptmode

This command disables the circuit ID option mode for BootP/DHCP Relay on the system.

Format	**no bootpdhcprelay cidoptmode**
Mode	Global Config

bootpdhcprelay enable

This command enables the forwarding of relay requests for BootP/DHCP Relay on the system.

Default	disabled
Format	**bootpdhcprelay enable**
Mode	Global Config

no bootpdhcprelay enable

This command disables the forwarding of relay requests for BootP/DHCP Relay on the system.

Format	**no bootpdhcprelay enable**
Mode	Global Config

bootpdhcprelay maxhopcount

This command configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system. The *<hops>* parameter has a range of 1 to 16.

Default	4
Format	**bootpdhcprelay maxhopcount** *<1-16>*
Mode	Global Config

no bootpdhcprelay maxhopcount

This command configures the default maximum allowable relay agent hops for BootP/DHCP Relay on the system.

Format	**no bootpdhcprelay maxhopcount**
Mode	Global Config

bootpdhcprelay minwaittime

This command configures the minimum wait time in seconds for BootP/DHCP Relay on the system. When the BOOTP relay agent receives a BOOTREQUEST message, it MAY use the seconds-since-client-began-booting field of the request as a factor in deciding whether to relay the request or not. The parameter has a range of 0 to 100 seconds.

Default	0
Format	**bootpdhcprelay minwaittime** *<0-100>*
Mode	Global Config

no bootpdhcprelay minwaittime

This command configures the default minimum wait time in seconds for BootP/DHCP Relay on the system.

Format	`no bootpdhcprelay minwaittime`
Mode	Global Config

show bootpdhcprelay

This command displays the BootP/DHCP Relay information.

Format	`show bootpdhcprelay`
Modes	• Privileged EXEC • User EXEC

Term	*Definition*
Maximum Hop Count	The maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	The minimum wait time.
Admin Mode	Indicates whether relaying of requests is enabled or disabled.
Server IP Address	The IP address for the BootP/DHCP Relay server.
Circuit Id Option Mode	The DHCP circuit Id option which may be enabled or disabled.
Requests Received	The number or requests received.
Requests Relayed	The number of requests relayed.
Packets Discarded	The number of packets discarded.

IP HELPER COMMANDS

This section describes the commands to configure a DHCP relay agent with multiple DHCP server addresses per routing interface, and to use different server addresses for client packets arriving on different interfaces on the relay agent.

ip helper-address

Use this command to add a unicast helper address to the list of helper addresses on an interface. This is the address of a DHCP server. This command can be applied multiple times on the routing interface to form the helper addresses list until the list reaches the maximum supported helper addresses.

Format	`ip helper-address <ip-address>`
Mode	Interface Config

no ip helper-address

Use this command to remove the IP address from the previously configured list. The no command without an <ip-address> **argument removes the entire list of helper addresses on that interface.**

Format	**no ip helper-address <ip-address>**
Mode	Interface Config

show ip helper-address

Use this command to display the configured helper addresses on the given interface.

Format	**show ip helper-address** *<interface>*
Mode	• Privileged EXEC • User EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show ip helper-address 0/1

Helper IP Address.............................. 1.2.3.4
.............................................. 1.2.3.5
```

ROUTING INFORMATION PROTOCOL COMMANDS

This section describes the commands you use to view and configure Routing Information Protocol (RIP), which is a distance-vector routing protocol that you use to route traffic within a small network.

router rip

Use this command to enter Router RIP mode.

Format	**router rip**
Mode	Global Config

enable (RIP)

This command resets the default administrative mode of RIP in the router (active).

Default	enabled
Format	**enable**
Mode	Router RIP Config

no enable (RIP)

This command sets the administrative mode of RIP in the router to inactive.

Format	`no enable`
Mode	Router RIP Config

ip rip

This command enables RIP on a router interface.

Default	disabled
Format	`ip rip`
Mode	Interface Config

no ip rip

This command disables RIP on a router interface.

Format	`no ip rip`
Mode	Interface Config

auto-summary

This command enables the RIP auto-summarization mode.

Default	disabled
Format	`auto-summary`
Mode	Router RIP Config

no auto-summary

This command disables the RIP auto-summarization mode.

Format	`no auto-summary`
Mode	Router RIP Config

default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format	`default-information originate`
Mode	Router RIP Config

no default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format	**no default-information originate**
Mode	Router RIP Config

default-metric (RIP)

This command is used to set a default for the metric of distributed routes.

Format	**default-metric** <*0-15*>
Mode	Router RIP Config

no default-metric (RIP)

This command is used to reset the default metric of distributed routes to its default value.

Format	**no default-metric**
Mode	Router RIP Config

distance rip

This command sets the route preference value of RIP in the router. Lower route preference values are preferred when determining the best route. A route with a preference of 255 cannot be used to forward traffic.

Default	15
Format	**distance rip** <*1-255*>
Mode	Router RIP Config

no distance rip

This command sets the default route preference value of RIP in the router.

Format	**no distance rip**
Mode	Router RIP Config

distribute-list out (RIP)

This command is used to specify the access list to filter routes received from the source protocol.

Default	0
Format	**distribute-list** <*1-199*> **out** {*static	connected*}
Mode	Router RIP Config

no distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Format	**no distribute-list** *<1-199>* **out** *{static | connected}*
Mode	Router RIP Config

ip rip authentication

This command sets the RIP Version 2 Authentication Type and Key for the specified interface. The value of *<type>* is either *none*, *simple*, or *encrypt*. The value for authentication key [*key*] must be 16 bytes or less. The [*key*] is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. If the value of *<type>* is *encrypt*, a keyid in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID.

Default	none
Format	**ip rip authentication** *{none | {simple <key>} | {encrypt <key> <keyid>}}*
Mode	Interface Config

no ip rip authentication

This command sets the default RIP Version 2 Authentication Type for an interface.

Format	**no ip rip authentication**
Mode	Interface Config

ip rip receive version

This command configures the interface to allow RIP control packets of the specified version(s) to be received.

The value for *<mode>* is one of: *rip1* to receive only RIP version 1 formatted packets, *rip2* for RIP version 2, *both* to receive packets from either format, or *none* to not allow any RIP control packets to be received.

Default	both
Format	**ip rip receive version** *{rip1 | rip2 | both | none}*
Mode	Interface Config

no ip rip receive version

This command configures the interface to allow RIP control packets of the default version(s) to be received.

Format	**no ip rip receive version**
Mode	Interface Config

ip rip send version

This command configures the interface to allow RIP control packets of the specified version to be sent. The value for *<mode>* is one of: *rip1* to broadcast RIP version 1 formatted packets, *rip1c* (RIP version 1 compatibility mode) which sends RIP

version 2 formatted packets via broadcast, *rip2* for sending RIP version 2 using multicast, or *none* to not allow any RIP control packets to be sent.

Default	ripi2
Format	**ip rip send version** *{rip1 | rip1c | rip2 | none}*
Mode	Interface Config

no ip rip send version

This command configures the interface to allow RIP control packets of the default version to be sent.

Format	**no ip rip send version**
Mode	Interface Config

hostroutesaccept

This command enables the RIP hostroutesaccept mode.

Default	enabled
Format	**hostroutesaccept**
Mode	Router RIP Config

no hostroutesaccept

This command disables the RIP hostroutesaccept mode.

Format	**no hostroutesaccept**
Mode	Router RIP Config

split-horizon

This command sets the RIP split horizon mode. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are: None - no special processing for this case. Simple - a route will not be included in updates sent to the router from which it was learned. Poisoned reverse - a route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity.

Default	simple
Format	**split-horizon** *{none | simple | poison}*
Mode	Router RIP Config

no split-horizon

This command sets the default RIP split horizon mode.

Format	**no split-horizon**
Mode	Router RIP Config

redistribute (RIP)

This command configures RIP protocol to redistribute routes from the specified source protocol/routers. There are five possible match options. Internal routes are redistributed by default.

Default	• metric—not-configured • match—internal
Format for source protocol	**redistribute** *{static | connected} [metric <0-15>]*
Mode	Router RIP Config

no redistribute

This command de-configures RIP protocol to redistribute routes from the specified source protocol/routers.

Format	**no redistribute** *{static | connected} [metric] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]*
Mode	Router RIP Config

show ip rip

This command displays information relevant to the RIP router.

Format	**show ip rip**
Modes	• Privileged EXEC • User EXEC

Term	*Definition*
RIP Admin Mode	Enable or disable.
Split Horizon Mode	None, simple or poison reverse.
Auto Summary Mode	Enable or disable. If enabled, groups of adjacent routes are summarized into single entries, in order to reduce the total number of entries The default is enable.
Host Routes Accept Mode	Enable or disable. If enabled the router accepts host routes. The default is enable.
Global Route Changes	The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.
Global queries	The number of responses sent to RIP queries from other systems.
Default Metric	The default metric of redistributed routes if one has already been set, or blank if not configured earlier. The valid values are 1 to 15.
Default Route Advertise	The default route.

show ip rip interface brief

This command displays general information for each RIP interface. For this command to display successful results routing must be enabled per interface (i.e., ip rip).

Format `show ip rip interface brief`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
IP Address	The IP source address used by the specified RIP interface.
Send Version	The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2
Receive Version	The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both
RIP Mode	The administrative mode of router RIP operation (enabled or disabled).
Link State	The mode of the interface (up or down).

show ip rip interface

This command displays information related to a particular RIP interface.

Format `show ip rip interface` *<slot/port>*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash. This is a configured value.
IP Address	The IP source address used by the specified RIP interface. This is a configured value.
Send Version	The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2. This is a configured value.
Receive Version	The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both. This is a configured value.
Both RIP Admin Mode	RIP administrative mode of router RIP operation; enable activates, disable de-activates it. This is a configured value.
Link State	Indicates whether the RIP interface is up or down. This is a configured value.
Authentication Type	The RIP Authentication Type for the specified interface. The types are none, simple, and encrypt. This is a configured value.
Default Metric	A number which represents the metric used for default routes in RIP updates originated on the specified interface. This is a configured value.

The following information will be invalid if the link state is down.

Term	*Definition*
Bad Packets Received	The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.
Bad Routes Received	The number of routes contained in valid RIP packets that were ignored for any reason.
Updates Sent	The number of triggered RIP updates actually sent on this interface.

ICMP THROTTLING COMMANDS

This section describes the commands you use to configure options for the transmission of various types of ICMP messages.

ip unreachables

Use this command to enable the generation of ICMP Destination Unreachable messages. By default, the generation of ICMP Destination Unreachable messages is enabled.

Default enable

Format `ip unreachables`

Mode Interface Config

no ip unreachables

Use this command to prevent the generation of ICMP Destination Unreachable messages.

Format `no ip unreachables`

Mode Interface Config

ip redirects

Use this command to enable the generation of ICMP Redirect messages by the router. By default, the generation of ICMP Redirect messages is enabled.

Default enable

Format `ip redirects`

Mode
- Global Config
- Interface Config

no ip redirects

Use this command to prevent the generation of ICMP Redirect messages by the router.

Format `no ip redirects`

Mode
- Global Config
- Interface Config

ip icmp echo-reply

Use this command to enable the generation of ICMP Echo Reply messages by the router. By default, the generation of ICMP Echo Reply messages is enabled.

Default	enable
Format	`ip icmp echo-reply`
Mode	Global Config

no ip icmp echo-reply

Use this command to prevent the generation of ICMP Echo Reply messages by the router.

Format	`no ip icmp echo-reply`
Mode	Global Config

ip icmp error-interval

Use this command to limit the rate at which IPv4 ICMP error messages are sent. The rate limit is configured as a token bucket, with two configurable parameters, *burst-size* and *burst-interval*.

The *burst-interval* specifies how often the token bucket is initialized with *burst-size* tokens. *burst-interval* is from 0 to 2147483647 milliseconds (msec).

The *burst-size* is the number of ICMP error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages.

To disable ICMP rate limiting, set *burst-interval* to zero (0).

Default	• *burst-interval* of 1000 msec. • *burst-size* of 100 messages
Format	`ip icmp error-interval` <*burst-interval*> *[<burst-size>]*
Mode	Global Config

no ip icmp error-interval

Use the **no** form of the command to return *burst-interval* and *burst-size* to their default values.

Format	`no ip icmp error-interval`
Mode	Global Config

Section 5: Wireless Commands

This section describes the CLI commands you use to manage the wireless features on the switch as well as the wireless access points that a switch manages.

This section contains the following subsections:

The commands in this section are in one of three functional groups:

- **Show** commands display switch settings, statistics and other information.
- **Configuration** Commands configure features and options. For every configuration command there is a show command that displays the configuration setting.
- **Clear** commands clear some or all of the settings to factory defaults.

UNIFIED SWITCH COMMANDS

The commands in this section provide global Unified Switch configuration, status, and statistics.

wireless

This command enters the Unified Switch global configuration mode.

Format	**wireless**
Mode	Global Config

enable (Wireless Config Mode)

This command enables the Unified Switch functionality.

Default	Enable
Format	**enable**
Mode	Wireless Config

no enable

The **no** version of this command disables the Unified Switch functionality.

Format	**no enable**
Mode	Wireless Config

country-code

This command globally configures the country code for the Unified 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. The **show country-code** command displays all valid country codes.

Default	US
Format	**country-code** *<code>*
Mode	Wireless Config

Parameter	*Description*
code	This parameter must identify a valid country code.

Example: The following shows an example of the command.

```
(DWS-4026) (Config wireless)# country-code au <cr>
Are you sure you want to change the country code? (y/n)
```


no country-code

The **no** version of this command returns the configured country code to the default.

Format **no country-code**
Mode Wireless Config

OUI database

This command adds a new entry to the OUI database, if not already present. Each entry consists of an OUI Value, which is composed of the higher three octets of the Ethernet MAC address of the AP/Client and the organization name for the OUI, which is a 32-byte string.

Format **oui database** *<ouival> <oui>*
Mode Wireless Config Mode

Parameter	*Description*
ouival	OUI Value of the vendor of AP/Client.
oui	Organization name for the OUI.

Example: The following example adds an OUI entry with the value and vendor name as shown.

```
DWS-4026 (Config-wireless)# oui database 00:00:01 "VendorName"
```

no OUI database

The **no** version of this command deletes the OUI entry for the specified OUI Value from the local OUI database.

Format **no oui database** *<ouival>*
Mode Wireless Config Mode

peer-group

This command indicates 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.

Default 1
Format **peer-group** *<1-255>*
Mode Wireless Config

Parameter	*Description*
1-255	The identifier for the peer switch group. The range is from 1 to 255.

no peer-group

The **no** version of this command returns the configured peer switch group to the default.

Format	**no peer-group**
Mode	Wireless Config

discovery method

This command enables various methods used for the discovery of APs and peer switches. If no method is specified, then it enables all the discovery methods.

Default	IP-Polling – Enable, L2-Multicast - Enable
Format	**discovery method** *[{ip-poll | l2-multicast}]*
Mode	Wireless Config

Parameter	*Description*
ip-poll	Enable IP-based discovery of APs and peer switches.
l2-multicast	Enable L2-based discovery of APs and peer switches.

no discovery method

The **no** version of this command disables the specified discovery method. If no method is specified, then it disables all the discovery methods.

Format	**no discovery method** *[{ip-poll | l2-multicast}]*
Mode	Wireless Config

discovery ip-list

This command adds an IP address to the list of addresses global to the Unified Switch. The switch polls each address in the list to discover new access points and peers. The list is used when discovery via IP polling is enabled.

Format	**discovery ip-list** *<ipaddr>*
Mode	Wireless Config

Parameter	*Description*
ipaddr	A valid IP address.

no discovery ip-list

The **no** version of this command deletes the specified IP address from the polling list. If an argument is not specified, all entries are deleted from the polling list.

Format `no discovery ip-list [<ipaddr>]`
Mode Wireless Config

discovery vlan-list

This command adds VLAN IDs on which to send L2 discovery multicast frames. Up to 16 VLAN IDs can be configured. By default, there is one entry in the list, 1 - Default VLAN.

Default 1 – Default VLAN
Format `discovery vlan-list <1-4094>`
Mode Wireless Config

Parameter	*Description*
1-4094	A VLAN ID in the range 1 to 4094.

no discovery vlan-list

The **no** version of this command deletes the VLAN ID from the discovery list. If no arguments are specified, all VLANs are deleted from the list except for the first entry. At least one entry must be configured in the list.

Format `no discovery vlan-list [<1-4094>]`
Mode Wireless Config

ap validation

This command configures whether to use the local valid AP database or a RADIUS server to validate newly discovered APs.

Default local
Format `ap validation {local | radius}`
Mode Wireless Config

Parameter	*Description*
local	Local database is used for validating discovered APs.
radius	RADIUS server is used for validating discovered APs.

ap authentication

This command enables AP authentication. When enabled, all APs are required to authenticate to the Unified Switch using a password upon discovery.

Default Disable
Format `ap authentication`
Mode Wireless Config

no ap authentication

The **no** version of this command disables AP authentication. APs are not required to authenticate to the Unified Switch upon discovery.

Format	**no ap authentication**
Mode	Wireless Config

ap client-qos

This command enables AP client QoS operation globally for the Unified 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: access control, bandwidth limiting, and differentiated services.

Note: This command takes effect in an AP without requiring that the AP profile be re-applied.

Default	Disable
Format	**ap client-qos**
Mode	Wireless Config

no ap client-qos

The **no** version of this command disables AP client QoS operation globally. Client traffic is not subject to QoS processing in any APs attached to this Unified Switch.

Format	**no ap client-qos**
Mode	Wireless Config

snmp-server enable traps wireless

This command globally enables the Unified Switch SNMP traps. The specific wireless trap groups are configured using the **trapflags** command in Wireless Config Mode.

Default	Disable
Format	**snmp-server enable traps wireless**
Mode	Global Config

no snmp-server enable traps wireless

The **no** version of this command globally disables all Unified Switch SNMP traps.

Format	**no snmp-server enable traps wireless**
Mode	Global Config

trapflags (Wireless Config Mode)

This command enables Unified Switch SNMP trap groups for wireless system events. If no parameters are specified, then all traps are enabled.

Default All - Disable

Format **trapflags** [{*ap-failure* | *ap-state* | *client-state* | *peer-ws* | *rf-scan* | *rogue-ap* | *ws-status*}]

Mode Wireless Config

Parameter	*Description*
ap-failure	Enable/Disable SNMP traps associated with AP association/authentication failures.
ap-state	Enable/Disable SNMP traps associated with AP state changes.
client-failure	Enable/Disable SNMP traps associated with client association/authentication failures.
client-state	Enable/Disable SNMP traps associated with client state changes.
peer-ws	Enable/Disable SNMP traps associated with peer Unified Switch events.
rf-scan	Enable/Disable SNMP traps associated with RF scan related events.
rogue-ap	Enable/Disable SNMP traps associated with rogue access points.
ws-status	Enable/Disable SNMP traps associated with wireless status events.
wids-status	Enable/Disable SNMP traps for WIDS status events.

no trapflags

The **no** version of this command disables Unified Switch SNMP trap groups for wireless system events. If no parameters are specified, then all traps are disabled.

Format **no trapflags** *[{ap-failure | ap-state | client-state | peer-ws | rf-scan | rogue-ap | ws-status}]*

Mode Wireless Config

agetime

This command configures database entry age times for the Unified Switch. A time value of 0 indicates entries in the corresponding database will not age and you must manually delete them.

Default 24 hours

Format **agetime** *{ad-hoc | ap-failure | client-failure | rf-scan |detected-client} <0,1-168>*

Mode Wireless Config

Parameter	*Description*
ad-hoc	Time in hours to maintain an entry in the ad hoc client network list.
ap-failure	Time in hours to maintain an entry in the AP association and authentication failure list.
client-failure	Time in hours to maintain an entry in the client association and authentication failure list.

Parameter	*Description*
rf-scan	Time in hours to maintain an entry obtained from an RF scan.
detected-client	Time in hours to maintain an entry in the detected clients database.
0,1-168	Time in hours from 0 to 168. A value of 0 indicates that entries should never age out.

no agetime

The **no** version of this command returns the configured entry age time to the default.

Format **no agetime** *{ad-hoc | ap-failure | client-failure | rf-scan |detected-client}*

Mode Wireless Config

peer-switch configuration

This command enables 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. If no parameters are specified, then all switch configuration groups are enabled.

Default
- ap-database - Enable
- ap-profile - Enable,
- captive-portal - Enable
- channel-power - Enable,
- discovery – Disable,
- global – Enable,
- known-client – Enable
- radius-client – Enable

Format `peer-switch configuration` *[{ap-database|ap-profile|captive-portal|channel-power|discovery|global|known-client|radius-client}]*

Mode Wireless Config

Parameter	*Description*
ap-database	Enable/Disable AP database configuration push to peer switches.
ap-profile	Enable/Disable AP profile and network configuration push to peer switches.
captive-portal	Enable/Disable Captive Portal configuration push to peer switches.
channel-power	Enable/Disable channel and power configuration push to peer switches.
discovery	Enable/Disable discovery configuration push to peer switches.
global	Enable/Disable global configuration push to peer switches.
known-client	Enable/Disable known client database push to peer switches.
radius-client	Enable/Disable RADIUS client configuration push to peer switches.

no peer-switch configuration

The **no** version of this command disables peer switch configuration for the wireless system. If no parameters are specified, then all peer switch configurations are disabled.

Format **no peer-switch configuration** [{ap-database|ap-profile|captive-portal| channel-power|discovery|global|known-client|radius-client}]

Mode Wireless Config

wireless peer-switch configure

This command allows the administrator to initiate a configuration push to one or all peer switches. If no parameters are given, all peer switches are configured. If the optional IP address parameter is specified, only that peer switch is configured.

Format **wireless peer-switch configure** *[<ipaddr>]*

Mode Privileged EXEC

Parameter	*Description*
ipaddr	Peer switch IP address.

client roam-timeout

This command configures maximum duration for which a client entry is retained in the client association database after disassociating from a managed AP. Roam-timeout is the time in seconds after disassociation for the entry to be deleted from the managed AP client association database.

Default 30 seconds

Format **client roam-timeout** *<1-120>*

Mode Wireless Config

Parameter	*Description*
roam-timeout	Time in seconds after disassociation for the entry to be deleted from the managed AP client association database.
1-120	Time in seconds from 1 to 120.

no client roam-timeout

The **no** version of this command returns the configured client age timeout to the default.

Format **no client roam-timeout**

Mode Wireless Config

tunnel-mtu

This command configures the network MTU size for all access points. This configuration is only used for tunneled networks and is, therefore, only available if the wireless tunneling feature is enabled. Note that the physical ports on the Unified Switch and the rest of the network devices must also be configured with the appropriate MTU size. This configuration applies only to the managed access points.

Default 1500

Format **tunnel-mtu** *{1500 | 1520}*

Mode Wireless Config

Parameter	*Description*
1500	Maximum IP frame size is 1518 tagged/1522 untagged.
1520	Maximum IP frame size is 1538 tagged/1542 untagged.

no tunnel-mtu

The **no** version of this command returns the configured network MTU size to the default value.

Format **no tunnel-mtu**

Mode Wireless Config

cluster-priority

This command configures 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.

Default 0

Format **cluster-priority** *<0-255>*

Mode Wireless Config

Parameter	*Description*
0-255	Preference level for Cluster Controller election.

radius server-name

This command configures global RADIUS authentication /accounting server name for wireless clients. The server name can contain alphanumeric characters plus –, _, and space.

Default
- Default-RADIUS-Server – authentication server name
- Default-RADIUS-Server – accounting server name

Format **radius server-name** *{auth | acct} <name>*

Mode Wireless Config

no radius server-name

The **no** version of this command sets the global RADIUS authentication /accounting server name to the default value.

Format **no radius server-name** {auth | acct}

Mode Wireless Config

Example: The following shows examples of the command.

```
(DWS-4026) #radius server-name auth  "Wireless_Auth-Server 1" ?
<cr>   Press Enter to execute the command.

(DWS-4026) #no radius server-name auth ?
<cr>   Press Enter to execute the command.

(DWS-4026) #radius server-name acct  "Wireless_Acct_Server 1" ?
<cr>   Press Enter to execute the command.

(DWS-4026) #no radius server-name acct  ?
<cr>   Press Enter to execute the command.
```

radius accounting (Wireless Config)

This command configures global RADIUS accounting mode for wireless clients.

Default	Disable
Format	**radius accounting**
Mode	Wireless Config

no radius accounting (Wireless Config)

The **no** version of this command disables global RADIUS accounting mode for wireless clients.

Format	**no radius accounting**
Mode	Wireless Config

Example: The following shows examples of the commands.

```
(DWS-4026) # radius accounting ?
<cr>   Press Enter to execute the command.

(DWS-4026) # no radius accounting ?
<cr>   Press Enter to execute the command
```

mac-authentication-mode

This command configures 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.

Default	white-list
Format	**mac-authentication-mode** *{white-list | black-list}*
Mode	Wireless Config

Parameter	*Description*
white-list	The access is granted only to clients with MACs in the Known Client database.
black-list	The access is denied to clients with MACs in the known client database.

known-client

This command configures a client MAC address in the local Known Client database. The action indicates whether to grant, deny, or use global action for MAC authentication of the client.

Format	**known-client** *<macaddr> [name <name>] [action {global-action | grant | deny}]*
Mode	Wireless Config

Parameter	*Description*
macaddr	A valid MAC address.
name	An alphanumeric string up to 32 characters in length.
global-action	Default authentication action is global-action. Apply global action to the client.
grant	Grant access to the client.
deny	Deny access to the client.

no known-client

The **no** version of this command deletes an entry from the local Known Client database.

Format	**no known-client** *<macaddr>*
Mode	Wireless Config

show wireless

This **show** command displays the configured Unified Switch global parameters and the operational status.

Format	**show wireless**
Mode	• Privileged EXEC • User EXEC

Field	*Description*
Administrative Mode	Shows whether the administrative mode is enabled.
WLAN Switch Operational Mode	Shows whether the wireless function on the switch is enabled.
WS IP Address	Shows the IP address of the switch. If the routing package is enabled, this address belongs to a routing or loopback interface.
AP Authentication Mode	Shows whether the AP must be authenticated by using the local database or a RADIUS database.
AP Auto Upgrade Mode	Shows whether the Auto Upgrade feature is enabled or disabled.
AP Validation Method	Shows whether to use the local or RADIUS server database for AP validation.
Client Roam Timeout (secs)	Shows how long to wait before a client that disassociates from this AP or a neighbor AP must re-authenticate when it associates again.

Field	*Description*
Country Code	Shows the country in which the WLAN is operating.
Peer Group ID	Shows the Peer group ID.
Cluster Priority	Priority of this switch for the Cluster election.
Cluster Controller	Indicates whether or not this switch is the Cluster controller.
Cluster Controller IP Address	The IP address of the switch that acts as the Cluster controller.
AP Client Qos Mode	Shows whether the AP Client QoS mode is enabled or disabled.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless

Administrative Mode.......................... Enable
WLAN Switch Operational Mode................. Enabled
WS IP Address................................ 10.0.0.1
AP Authentication Mode....................... Disable
AP Auto Upgrade Mode......................... Disable
AP Validation Method......................... Local
Client Roam Timeout (secs)................... 30
Country Code................................. US - United States
Peer Group ID................................ 1
Cluster Priority............................. 2
Cluster Controller........................... Yes
Cluster Controller IP Address................ 10.0.0.1
AP Client QoS Mode........................... Disable
```

show wireless country-code

This **show** command displays the country codes configurable on the Unified Switch.

Format **show wireless** country-code

Mode Privileged EXEC

Field	*Description*
Code	Shows the 2-letter country code.
Country	Shows the name of the country associated with the code.

show wireless OUI database

This **show** command displays all the OUI entries created by the admin in the local OUI database.

Format **show OUI database** *[<ouival>]*

Mode Privileged EXEC

Field	*Description*
ouival	OUI Value of the vendor of AP/Client.
oui	Organization name for the OUI.

Example:

```
OUI Value             OUI Description
--------------------  --------------------------------
00:11:11
00:11:12              Andreys OUI

(DWS-4026) #
```

show wireless discovery

This **show** command displays the configured Unified Switch discovery methods.

Format	**`show wireless discovery`**
Mode	Privileged EXEC

Field	*Description*
IP Polling Mode	Shows whether the L3 IP Polling discovery method is enabled.
L2 Multicast Discovery Mode	Shows whether the L2 Multicast Discovery Mode is enabled.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless discovery

IP Polling Mode ............................... Enabled
L2 Multicast Discovery Mode ................... Enabled
```

show wireless discovery ip-list

This **show** command displays the configured Unified Switch IP polling list and the polling status for each configured IP address for discovery.

Format	**`show wireless discovery ip-list`**
Mode	Privileged EXEC

Field	*Description*
IP Address	Shows the IP addresses configured in the L3/IP Discovery List.
Status	Shows the L3 discovery status. Possible values are *Not Polled*, *Unreachable*, or *Discovered*.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless discovery ip-list
```



```
IP Address       Status
---------------- ------------
1.1.1.1          Not Polled
```

show wireless discovery vlan-list

This **show** command displays the configured VLAN ID list for L2 discovery.

Format `show wireless discovery vlan-list`

Mode Privileged EXEC

Field	*Description*
VLAN	Shows the ID and name of each VLAN in the L2 Discovery list.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless discovery vlan-list

VLAN
----------------
- Default
```

show wireless status

This **show** command displays the configured global Unified Switch status parameters. The counters are aggregated for the peer group if the switch acts as Cluster Controller. If the switch is not a Cluster Controller, the values are for this switch only; however, the parameters that describe maximum limits are for the peer group.

Format `show wireless status`

Mode Privileged EXEC

Field	*Description*
Total Access Points	The total number of access points in the managed AP database. This value is always equal to the sum of Managed Access Points, Connection Failed Access Points, and Discovered Access Points.
Managed Access Points	The total number of APs in the managed AP database that are authenticated, configured, and have an active connection with the Unified Switch.
Connection Failed Access Points	The number of APs that were previously authenticated and managed, but lost connection with the Unified Switch.
Discovered Access Points	APs that have a connection with the switch, but have not yet been completely configured (i.e., managed APs with a discovered or authenticated status).
Maximum Managed APs in Peer Group	The total number of managed APs that the wireless system (peer group) supports.
Rogue AP Mitigation Count	Number of APs to which the wireless system is currently sending de-authentication messages to mitigate against rogue APs.
Rogue AP Mitigation Limit	Maximum number of APs for which the system can send de-authentication frames.
Total Clients	Total number of clients in the database. This total includes clients with an Associated, Authenticated, or Disassociated status.

Field	*Description*
Authenticated Clients	Total number of clients in the associated client database with an “Authenticated” status.
Maxumum Associated Clients	Maximum number of clients that can associate with the wireless system. This is the maximum number of entries allowed in the Associated Client database.
Detected Clients	The total number of detected clients in the database.
Maximum Detected Clients	The maximum number of detected clients that can be stored in the database.
Peer Switches	Total number of peer WLAN switches detected on the network.
Unknown Access Points	Total number of APs currently detected but not known to the switch. These includes rogue APs and APs not connected to the network.
Rogue Access Points	Total number of rogue APs currently detected on the WLAN.
Standalone Access Points	Total number of trusted APs in standalone mode.
Distributed Tunnel Clients	Number of clients that are currently sending and receiving packets via distributed tunnels.
WLAN Utilization	Total network utilization across all APs managed by this switch, this is an average of the global statistics received from each AP.
Maximum Pre-authentication History Entries	Maximum number of Client Pre-Authentication events that can be recorded by the system.
Total Pre-authentication History Entries	Current number of pre-authentication history entries in use by the system.
Maximum Roam History Entries	Maximum number of entries that can be recorded in the roam history for all detected clients.
Total Roam History Entries	Current number of roam history entries in use by the system.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #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............ 256
Rogue AP Mitigation Count.................... 0
Rogue AP Mitigation Limit.................... 16
Total Clients................................ 0
Authenticated Clients........................ 0
Maximum Associated Clients................... 8000
Detected Clients............................. 0
Maximum Detected Clients..................... 16000
Peer Switches................................ 1
Unknown Access Points........................ 0
Rogue Access Points.......................... 0
Standalone Access Points..................... 0
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
```

show wireless statistics

This **show** command displays the current global Unified Switch statistics. The counters are aggregated for the peer group the switch acts as the Cluster Controller for the group. If the switch is not the Cluster Controller, the values are for this switch only.

Format `show wireless statistics`

Mode Privileged EXEC

Field	*Description*
WLAN Bytes Received	Shows the total bytes received across all APs managed by the switch.
WLAN Bytes Transmitted	Shows the total bytes transmitted across all APs managed by the switch.
WLAN Packets Received	Shows the total number of packets received across all APs managed by the switch.
WLAN Packets Transmitted	Shows the total number of packets transmitted across all APs managed by the switch.
WLAN Bytes Received Dropped	Shows the total bytes received across all APs managed by the switch and dropped.
WLAN Bytes Transmit Dropped	Shows the total bytes transmitted across all APs managed by the switch and dropped.
WLAN Packets Receive Dropped	Shows the total number of packets received across all APs managed by the switch and dropped.
WLAN Packets Transmit Dropped	Shows the total number of packets transmitted across all APs managed by the switch and dropped.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless statistics <cr>
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
```

show wireless switch status

This **show** command displays the current global Unified Switch status parameters. If the Unified Switch is a Cluster Controller, then this command shows per-switch status parameters for all the switches in the wireless network. For the switch that is not acting as a Cluster Controller, only the local status parameters are displayed.

Format **show wireless switch** *<ipaddr>* **status**

Mode Privileged EXEC

The following table lists the command parameters

Parameter	*Description*
ipaddr	IP address of the Unified Switch in the wireless system.

The following table lists the output fields that display.

Field	*Description*
Switch IP Address	IP address of the Unified Switch or any peer switch in the wireless system.
Cluster Priority	Priority of this switch for the Cluster election.
Total Access Points	The total number of access points in the managed AP database. This value is always equal to the sum of Managed Access Points, Connection Failed Access Points, and Discovered Access Points.
Managed Access Points	The total number of APs in the managed AP database that are authenticated, configured, and have an active connection with the Unified Switch.
Connection Failed Access Points	The number of APs that were previously authenticated and managed, but lost connection with the Unified Switch.
Discovered Access Points	APs that have a connection with the Unified Switch, but have not yet been completely configured (i.e. managed APs with a discovered or authenticated status).
Maximum Managed Access Points	The maximum number of managed access points supported by the switch.
Total Clients	Total number of clients in the database. This total includes clients with an Associated, Authenticated, or Disassociated status.
Authenticated Clients	Total number of clients in the associated client database with an “Authenticated” status.
Distributed Tunnel Clients	Number of clients that are currently sending and receiving packets via distributed tunnels.
WLAN Utilization	Total network utilization across all APs managed by this switch, this is an average of the global statistics received from each AP.

Example: The following shows example CLI display output for the command.

If a network consists of two switches 192.168.37.60 and 192.168.37.61 respectively and former is the Cluster Controller, this command works differently at Cluster Controller and peer switch that is not acting as a Cluster Controller as follows.

On the Cluster Controller, it displays entries in the following format:

```
(DWS-4026) show wireless switch 10.27.65.8 status

Switch IP Address.............................. 10.27.65.8
Cluster Priority............................... 1
Total Access Points............................ 0
Managed Access Points.......................... 0
Connection Failed Access Points................ 0
Discovered Access Points....................... 0
Maximum Managed Access Points.................. 64
Total Clients.................................. 0
Authenticated Clients.......................... 0
```



```
Distributed Tunnel Clients..................... 0
WLAN Utilization............................... 0 %
```

On the switch that is not acting as a Cluster Controller the summary command displays entries in the following format:

```
(DWS-4026) #show wireless switch 192.168.37.60 status
Error! Only Cluster Controller can display the peer switch status parameters.

(DWS-4026) #show wireless switch 192.168.37.61 status
Switch IP Address ............................. 192.168.37.61
Cluster Priority............................... 1
Total Access Points............................ 5
Managed Access Points.......................... 3
Connection Failed Access Points................ 1
Discovered Access Points....................... 1
Total Clients.................................. 3
Associated Clients............................. 1
Authenticated Clients.......................... 2
Standalone Access Points....................... 0
WLAN Utilization............................... 10 %
```

show wireless switch statistics

This **show** command displays the current Unified Switch statistics. If the Unified Switch is a Cluster Controller, then this command shows per switch statistics for all the switches in the wireless system. For the switch that is not acting as a Cluster controller, only the local statistics are displayed.

Format **show wireless** *{<ipaddr>|local}* **statistics**

Mode Privileged EXEC

Field	*Description*
ipaddr	IP address of the Unified Switch in the wireless system.

Example: The following shows example CLI display output for the command.

If a network consists of two switches 192.168.37.60 and 192.168.37.61 respectively and former is the Cluster Controller, this command works differently at Cluster Controller and the peer switch which is not a Cluster Controller as follows.

On the Cluster Controller, it displays entries in the following format:

```
(DWS-4026) #show wireless switch 192.168.37.60 statistics <cr>

WLAN Bytes Received............................ 1873
WLAN Bytes Transmitted......................... 8234
WLAN Packets Received.......................... 233
WLAN Packets Transmitted....................... 435
WLAN Bytes Receive Dropped..................... 0
WLAN Bytes Transmit Dropped.................... 0
WLAN Packets Receive Dropped................... 0
WLAN Packets Transmit Dropped.................. 0

(DWS-4026) #show wireless switch 192.168.37.61 statistics <cr>

WLAN Bytes Received............................ 320
```

```
WLAN Bytes Transmitted..................... 560
WLAN Packets Received...................... 45
WLAN Packets Transmitted................... 78
WLAN Bytes Receive Dropped................. 0
WLAN Bytes Transmit Dropped................ 0
WLAN Packets Receive Dropped............... 0
WLAN Packets Transmit Dropped.............. 0
```

On the switch that is not acting as a Cluster Controller the summary command displays entries in the following format:

```
(DWS-4026) #show wireless switch 192.168.37.60 statistics <cr>
Error! Only ClusterController can display the peer switch statistics.
(DWS-4026) #show wireless switch 192.168.37.61 statistics <cr>

WLAN Bytes Received........................ 320
WLAN Bytes Transmitted..................... 560
WLAN Packets Received...................... 45
WLAN Packets Transmitted................... 78
WLAN Bytes Receive Dropped................. 0
WLAN Bytes Transmit Dropped................ 0
WLAN Packets Receive Dropped............... 0
WLAN Packets Transmit Dropped.............. 0
```

The local switch statistics can also be displayed using the following command format:

```
(DWS-4026) #show wireless switch local statistics <cr>

WLAN Bytes Received........................ 320
WLAN Bytes Transmitted..................... 560
WLAN Packets Received...................... 45
WLAN Packets Transmitted................... 78
WLAN Bytes Receive Dropped................. 0
WLAN Bytes Transmit Dropped................ 0
WLAN Packets Receive Dropped............... 0
WLAN Packets Transmit Dropped.............. 0
```

show wireless trapflags

This **show** command displays the configured Unified Switch SNMP trap modes.

Format	**`show wireless trapflags`**
Mode	Privileged EXEC

Field	*Description*
AP Failure Traps	Shows whether AP Failure Traps are enabled.
AP State Change Traps	Shows whether AP State Change Traps are enabled.
Client Failure Traps	Shows whether Client Failure Traps are enabled.
Client State Change Traps	Shows whether Client State Change Traps are enabled.
Peer Switch Traps	Shows whether Peer Switch Traps are enabled.

Field	*Description*
RF Scan Traps	Shows whether RF Scan Traps are enabled.
Rogue AP Traps	Shows whether Rogue AP Traps are enabled.
WIDS Status Traps	Shows whether WIDS Status Traps are enabled.
Wireless Status Traps	Shows whether Wireless Status Traps are enabled.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless trapflags
AP Failure Traps.............................. Disable
AP State Change Traps......................... Disable
Client Failure Traps.......................... Disable
Client State Change Traps..................... Disable
Peer Switch Traps............................. Disable
RF Scan Traps................................. Disable
Rogue AP Traps................................ Disable
WIDS Status Traps............................. Disable
Wireless Status Traps......................... Disable
```

show trapflags (modified command)

The existing Unified Switch **show trapflags** command is modified to show the global Unified Switch trap configuration. See the command "show trapflags" on page 503.

show wireless tunnel-mtu

This **show** command displays the configured network MTU size. This is a global configuration for all managed access points.

Format	`show wireless tunnel-mtu`
Mode	Privileged EXEC

show wireless agetime

This **show** command displays the configured age times for the status database entries.

Format	`show wireless agetime`
Mode	Privileged EXEC

Field	*Description*
Ad Hoc Client Status Age (hours)	Shows how long to continue to display an ad hoc client in the status list since it was last detected.
AP Failure Status Age (hours)	Shows how long to continue to display a failed AP in the status list since it was last detected.
RF Scan Status Age (hours)	Shows how long to continue to display an AP detected through the RF Scan since it was last detected.
Detected Clients Age (hours)	Shows how long to keep an entry in the Detected Client Status list.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless agetime <cr>
Ad Hoc Client Statue Age (hours)..... 24
AP Failure Status Age (hours)..... 24
RF Scan Status Age (hours)..... 24
Detected Clients Age (hours).....24
```

show wireless peer-switch configuration

This show command displays the peer switch configuration groups mode.

Format	**show wireless peer-switch configuration**
Mode	Privileged EXEC

Field	*Description*
AP Database	Displays whether the AP database configuration push to peer switches is enabled or disabled.
AP Profile	Displays whether the AP profile and network configuration push to peer switches is enabled or disabled.
Channel Power	Displays whether the channel and power configuration push to peer switches is enabled or disabled.
Discovery	Displays whether the discovery configuration push to peer switches is enabled or disabled.
Global	Displays whether the global configuration push to peer switches is enabled or disabled.
Known Client	Displays whether the known client database push to peer switches is enabled or disabled.
Captive Portal	Displays whether Captive Portal configuration push to peer switches is enabled or disabled.
Radius Client	Displays whether RADIUS client configuration push to peer switches is enabled or disabled.
QoS ACL	Displays whether QoS ACL configuration push to peer switches is enabled or disabled.
QoS DiffServ	Displays whether QoS Diffserv (classes, services, and policies) configuration has been enabled to push the configuration to peer switches.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless peer-switch configuration

AP Database..................................... Enable
AP Profile...................................... Enable
Channel Power................................... Enable
Discovery....................................... Disable
Global.......................................... Enable
Known Client.................................... Enable
Captive Portal.................................. Enable
RADIUS Client................................... Enable
QoS ACL......................................... Enable
QoS DiffServ.................................... Enable
```

show wireless configuration request status

This show command displays the global peer switch configuration push status and configuration push status for all peer switches.

Format `show wireless configuration request status`

Mode Privileged EXEC

Field	*Description*
Status	The global status for the configuration push request.
Total Count	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	Indicates the total number of peer switches to which the configuration has been pushed successfully for the current configuration push request.
Failure Count	Indicates the total number of peer switches to which the configuration push request failed for the current configuration push request.
IP Address	The peer switch IP Address.
Configuration Status	Configuration push status for the peer switch.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless configuration request status
Global Status:
Configuration Status.................. Sending Configuration
Total Count         .................. 3
Success Count  ....................... 0
Failure Count ........................ 1

Peer-Switch Status:
IP Address         Configuration Status
---------------    --------------------
10.0.0.100         Failure Invalid Code Version
10.0.0.101         In Progress
10.0.0.102         Requested
```

show wireless configuration receive status

This show command displays the peer switch configuration received status.

Format `show wireless configuration receive status`

Mode Privileged EXEC

Field	*Description*
Switch IP	The peer switch IP address that pushed configuration.
Configuration Received	Indicates the configuration groups received as part of the configuration push.
Receive Time	Indicates the configuration push received time.
Receive Status	Indicates the status of the configuration push receive from the peer switch.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless configuration receive status

Switch IP.........................  192.168.30.20
Configuration Received ............AP Database,
                                   AP Profile,
                                   Channel Power,
                                   Discovery,
                                   Global,
                                        Known-Client
Receive Time ......................JAN 03 23:32:06 1970
Receive Status ....................Failure Invalid Configuration
```

show wireless ap capability

This command displays access point hardware type and radio hardware type capabilities. If no parameters are specified, a summary of access point hardware type capabilities for all supported AP hardware types is displayed. If an AP hardware type ID and radio interface is specified, the detailed hardware type capabilities are displayed. Note that in this release, only hardware type hw_dwl8600 is suported.

Format **show wireless ap capability** *[hw_dwl8600 radio <1-2>]*

Mode Privileged EXEC

Field	*Description*
hw_dwl8600	The AP hardware type ID.
<1-2>	The radio index on the AP hardware type.
Hardware Type ID	AP hardware type that supports this radio.
Hardware Type Description	Descriptive name of the AP hardware type.
Radio Count	Number of radios supported on the AP.
Image Type	AP image type ID and description.
Radio	The radio index of this radio in the AP.
Radio Type Description	Text description of this radio type.
VAP Count	Number of virtual access points supported by this radio.
802.11a Support	Flag indicating whether this radio supports 802.11a Mode.
802.11bg Support	Flag indicating whether this radio supports 802.11bg Mode.
802.11n Support	Flag indicating whether this radio supports 802.11n configuration parameters.

```
(DWS-4026) #show wireless ap capability

Hardware    Hardware                                Radio  VAP Count  Image
Type ID     Type Description                        Count  Per Radio  Type
--------    --------------------------------------- -----  ---------  --------
hw_dw18600  DWL-8600AP Dual Radio a/b/g/n           2      16         img_dwl8600

(DWS-4026) #
```



```
(DWS-4026) #show wireless ap capability hw_dwl8600 radio 2
Hardware Type.................................. DWL-8600AP Dual Radio a/b/g/n
Radio Count.................................... 2
Image Type..................................... DWL-8600AP Image

Radio.......................................... 2
Radio Type Description......................... D-Link Enterprise b/g/n
VAP Count...................................... 16
802.11a Support................................ Disable
802.11bg Support............................... Enable
802.11n Support................................ Enable
```

show wireless ap capability image-table

This command displays the access point image capability table.

Format **show wireless ap capability image-table**

Mode Privileged EXEC

Field	*Description*
Image Type ID	AP image type ID.
Image Type Description	Descriptive name of the AP image type.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless ap capability image-table

Image Type ID   Image Type Description
--------------  ----------------------
hw_dwl8600      DWL-8600AP image
```

show wireless radius

This show command displays the configured global RADIUS configuration for wireless clients.

Format **show wireless radius**

Mode Privileged EXEC

Field	*Description*
RADIUS Authentication Server Name	The name of the RADIUS server used for AP authentications as well as client authentications when a network-level RADIUS server is not defined.
RADIUS Authentication Server Configured	Indicates whether the specified named RADIUS Authentication server is configured in the RADIUS Client configuration.

Field	*Description*
RADIUS Accounting Server Name	The name of the RADIUS server used for reporting wireless client associations and disassociations when a network-level RADIUS accounting server is not defined.
RADIUS Accounting Server Configured	Indicates whether the specified named RADIUS Accounting server is configured in the RADIUS Client configuration.
RADIUS Accounting	Flag to indicate whether or not RADIUS accounting is enabled for wireless clients accounting.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless radius
RADIUS Authentication Server Name.......... Default-RADIUS-Server
RADIUS Authentication Server Configured.... Configured
RADIUS Accounting Server Name ............. Default-RADIUS-Server
RADIUS Accounting Server Configured........ Not Configured
RADIUS Accounting ......................... Disable
```

show wireless mac-authentication-mode

This show command displays the configured client MAC authentication mode for the switch.

Format **`show wireless mac-authentication-mode`**

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) # show wireless mac-authentication-mode
MAC Authentication Action..................... white-list
```

show wireless known-client

This show command displays the content of the local Known Client database or an entry of the local Know Client database.

Format **`show wireless known-client`** *`[<macaddr>]`*

Mode Privileged EXEC

Field	*Description*
MAC Address	The client MAC address in the local Known Client database.
Nickname	An alphanumeric string up to 32 characters in length.
Action	Indicates whether to grant, deny, or use global action for MAC authentication of the client.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless known-client

MAC Address          Nickname     Action
-------------------------------------------------
10:10:10:10:10:10    client1      grant
```


clear wireless statistics

This **clear** command resets the global Unified Switch statistics.

Format	**clear wireless statistics**
Mode	Privileged EXEC

Example: The following shows an example of the command.

```
(DWS-4026) #clear wireless statistics
Are you sure you want to clear the wireless switch statistics? (y/n)y
Sent clear statistics request to the wireless switch.
The statistics are not cleared immediately.

(DWS-4026) #clear wireless statistics
Are you sure you want to clear the wireless switch statistics? (y/n)n
Wireless switch statistics not cleared.
```

wireless acknowledge-rogue

Use this command to clear the rogue AP state in the RF Scan database for the specified AP. If you do not specify a MAC address, the rogue AP state will be cleared for all rogue APs.

Format	**wireless acknowledge-rogue** *[<macaddr>]*
Mode	Privileged Exec

dist-tunnel idle-timeout

Use this command to globally configure the time interval for which L2 distributed tunneled clients can stay idle. Beyond this time interval, the tunnel is terminated. The parameter idle-timeout is a numeric value in seconds.

Default	120
Format	**dist-tunnel idle-timeout** *<30-3600>*
Mode	Wireless Config

Parameter	*Description*
idle-timeout	The identifier for idle-timeout. The range is 30 to 3600 seconds.

dist-tunnel max-timeout

Use this command to globally configure the maximum time for the L2 distributed tunneled clients beyond which the tunnel is terminated. The parameter max-timeout is a numeric value in seconds.

Default	7200
Format	**dist-tunnel max-timeout** *<30-86400>*
Mode	Wireless Config

Parameter	*Description*
max-timeout	The identifier for max-timeout. The range is 30 to 86400 seconds.

dist-tunnel mcast-repl

Use this command to globally configure the maximum multicast replications allowed for the L2 distributed tunneled clients. The parameter mcast-repl is a numeric value.

Default 128

Format **dist-tunnel mcast-repl** *<1-1024>*

Mode Wireless Config

Parameter	*Description*
mcast-repl	The identifier for multicast replications. The range is 1 to 1024.

dist-tunnel max-clients

Use this command to globally configure the maximum number of clients that can be tunneled using L2 distributed tunnels. The parameter max clients value is a numeric value.

Default 128

Format **dist-tunnel max-clients** *<1-8000>*

Mode Wireless Config

Parameter	*Description*
max-clients	The identifier for maximum clients. The range is 1 to 8000.

UNIFIED SWITCH CHANNEL AND POWER COMMANDS

The commands in this section provide status and configuration for automatic channel planning and power adjustment.

channel-plan mode

This command configures the channel plan mode for each 802.11a/n and 802.11b/g/n frequency band. If it is *<interval>*, a channel plan is computed and applied at every defined interval. If it is *<manual>*, you must start and apply the channel plan manually. If it is *<time>*, then the channel plan will be computed and applied at the scheduled time.

Default manual

Format **channel-plan** *{an | bgn}* **mode** *{interval | manual | time}*

Mode Wireless Config

Parameter	*Description*
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
interval	Compute and apply new channel plans at the configured interval.
manual	Compute and apply new channel plans only when requested via the UI.
time	Compute and apply a new channel plan at the configured time.

channel-plan interval

This command configures the channel plan interval for each 802.11a/n and 802.11b/g frequency band. When the corresponding channel plan mode is configured for **interval**, this parameter indicates how often new channel plans are computed and applied.

Default 6

Format **channel-plan** *{an | bgn}* **interval** *<6-24>*

Mode Wireless Config

Parameter	*Description*
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
6-24	The channel plan interval in hours.

no channel-plan interval

The **no** version of this command returns the configured channel plan interval to the default.

Format **no channel-plan** *{an | bgn}* **interval**

Mode Wireless Config

channel-plan time

This command configures the channel plan time for each 802.11a/n and 802.11b/g/n frequency band. When the corresponding channel plan mode is configured for time, this parameter indicates the time of day a new channel plan is computed and applied.

Default	00:00
Format	**channel-plan** *{an | bgn}* **time** *<hh:mm>*
Mode	Wireless Config

Parameter	*Description*
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
hh:mm	The channel plan time in 24 hour time.

Example: The following shows an example of the command.

```
DWS-4026 (Config wireless)# channel-plan an time 23:59 ?
<cr>   Press Enter to execute the command.
```

no channel-plan time

The **no** version of this command returns the configured channel plan time to the default.

Format	**channel-plan** *{an | bgn}* **time**
Mode	Wireless Config

channel-plan history-depth

This command configures the number of channel plan history iterations that are maintained for each 802.11a/n and 802.11b/g/n frequency band. The number of iterations stored for each channel plan affects channel assignment; the channel algorithm will not assign the same channel to an AP more than once within the number of stored iterations of the channel plan.

Default	5
Format	**channel-plan** *{an | bgn}* **history-depth** *<0-10>*
Mode	Wireless Config

Parameter	*Description*
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
0-10	Channel plan history depth.

no channel-plan history-depth

The **no** version of this command returns the history depth for the channel plan to the default.

Format **no channel-plan** *{an | bgn}* **history-depth**
Mode Wireless Config

power-plan mode

This command configures the power plan mode for managed APs. If it is *<interval>*, power adjustments are computed and applied at every defined interval. If it is *<manual>*, you must start and apply proposed power adjustments manually.

Default manual
Format **power-plan mode** *{interval | manual}*
Mode Wireless Config

Parameter	*Description*
interval	Compute and apply power adjustments at the configured interval.
manual	Compute and apply power adjustments only when requested via the UI.

power-plan interval

This command configures the power adjustment interval. When the power plan mode is configured for **interval**, this parameter indicates how often new power adjustments are computed and applied.

Default 4
Format **power plan interval** *<1-24>*
Mode Wireless Config

Parameter	*Description*
1-24	The power plan interval in hours.

no power-plan interval

The **no** version of this command returns the configured power adjustment interval to the default.

Format **no power-plan interval**
Mode Wireless Config

wireless channel-plan

This command allows you to request manual channel plan actions for each 802.11n and 802.11b/g/n frequency band.

Format **wireless channel-plan** *{an | bgn} [peer group] {apply | clear | start}*
Mode Privileged EXEC

Parameter	*Description*
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
peer group	Run the channel plan for the entire peer-group.
apply	Apply the entire proposed channel plan.
clear	Clear the current proposed channel plan.
start	Compute a new proposed channel plan.

wireless power-plan

This command allows you to manage manual power adjustments for the managed APs.

Format `wireless power-plan [peer group] {apply | clear | start}`

Mode Privileged EXEC

Parameter	*Description*
peer group	Run the power plan for the entire peer-group.
apply	Apply the proposed power adjustments.
clear	Clear the proposed power adjustments.
start	Compute new proposed power adjustments.

show wireless channel-plan

This command displays configuration for automatic channel planning. The channel plan type argument must be specified, the configuration and status is maintained separately for each radio frequency.

Format `show wireless channel-plan {an | bgn}`

Mode Privileged EXEC

Field	*Description*
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
Channel Plan	The channel plan type or mode, managed AP radios operating in the specified mode will be considered for this channel plan.
Channel Plan Mode	The frequency for automatic channel planning manual, fixed time, or interval. If the mode is manual, the channel algorithm will not run unless you request it.
Channel Plan Interval	If the channel plan mode is interval, this indicates the frequency in hours that the channel plan is computed and applied.
Channel Plan Fixed Time	If the channel plan mode is fixed time, this indicates the time (24-hour time) at which the channel plan is computed and applied.
Channel Plan History Depth	This indicates the number of iterations of the channel plan that are maintained in the channel plan history. The channel on a managed AP radio will not be changed more than once within the channel plan history.

show wireless channel-plan history

This command displays a history for the automatic channel algorithm. The channel plan type argument must be specified. A channel history is maintained separately for each radio frequency. The channel algorithm maintains a configured number of iterations of applied channel changes to avoid frequent channel changes to the same managed AP radio. If the IP address is not entered, the command displays a history summary for all peer switches. If a peer switch IP address is entered, detailed history for that peer switch is displayed.

Format **show wireless channel-plan history** *{an | bgn} [<ipaddr>]*

Mode Privileged EXEC

Field	*Description*
ipaddr	The *<ipaddr>* is a valid IP address.
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
Current Iteration	Indicates the current iteration of the channel plan.
Operational Status	Indicates whether automatic channel planning is active or inactive. Automatic channel planning may be inactive due to 802.11h or unsupported clear channels.
Last Algorithm Time	Indicates the last time the channel planning algorithm completed.
AP MAC address	The managed AP Ethernet MAC address.
Location	A descriptive location string configured for the managed AP.
Radio	The radio interface on the managed AP.
Iteration	Iteration of the channel plan where the new channel was computed and applied.
Channel	The channel computed and applied to the managed AP.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless channel-plan history a

Switch           Current        Last Algorithm
IP Address       Iteration      Time
--------------   --------       --------------
10.0.0.1         2              JAN 03 23:32:06 1970
10.254.22.1      3              JAN 03 23:33:06 1970
10.254.22.15     1              JAN 03 23:32:06 1970
10.254.22.16     0              --


Switch) #show wireless channel-plan history a 10.254.22.15
Switch IP Address..............................10.254.22.15
Current Iteration..............................0
Operational Status.............................Active

Last Algorithm Time...........................JAN 03 23:32:06 1970

AP MAC Address    Location             Radio  Iteration Channel
----------------- -------------------- ------ --------- -------
00:00:85:00:50:00 Third floor          1      1         6
```

show wireless channel-plan proposed

This command displays the proposed channel plan changes for a manual request to run the channel algorithm. The channel plan type argument must be specified. The channel algorithm is run separately for each radio frequency. The proposed channel changes may be cleared or applied using the **wireless channel-plan** command. If the IP address is not entered, the command displays a proposed summary for all peer switches. If a peer switch IP address is entered, detailed proposed entries for that peer switch are displayed.

Format **show wireless channel-plan proposed** *{an | bgn} [<ipaddr>]*

Mode Privileged EXEC

Field	*Description*
ipaddr	The *<ipaddr>* is a valid IP address.
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
Current Status	Indicates the status of a manual channel plan request.
AP MAC Address	The managed AP Ethernet MAC address.
Location	A descriptive location string configured for the managed AP.
Radio	The radio interface on the managed AP.
Current Channel	The current channel on the managed AP radio.
New Channel	The new channel computed by the channel algorithm.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless channel-plan proposed a


Switch IP Address       Current Status
------------------      ---------------
10.0.0.1                Apply Complete
10.254.22.1             Apply Complete
10.254.22.15            Apply Complete

(DWS-4026) #show wireless channel-plan proposed a 10.254.22.15
Current Status.............................. Apply Complete

                                                    Current New
AP MAC Address   Location                    Radio Channel Channel
---------------- --------------------------- ----- ------- -------
00:00:85:00:50:00 Third floor                 1     11      1
```

show wireless power-plan

This command displays status and configuration for automatic power adjustment. The command does not accept any arguments.

Format **show wireless power-plan**

Mode Privileged EXEC

Field	*Description*
Power Plan Mode	The mode for automatic power adjustment, manual or interval. If the mode is manual, the power algorithm will not run unless you request it.
Power Plan Interval	If the power adjustment mode is interval, this indicates the frequency in minutes that power adjustments are computed and applied.

show wireless power-plan proposed

This command displays the proposed power adjustments for a manual request to run the power algorithm. The command does not accept any arguments. The proposed power changes may be cleared or applied using the **wireless power-plan** command. If the IP address is not entered, the command displays a proposed summary for all peer switches. If a peer switch IP address is entered, detailed proposed entries for that peer switch are displayed.

Format **show wireless power-plan proposed** *[<ipaddr>]*

Mode Privileged EXEC

Field	*Description*
ipaddr	The *<ip addr>* is a valid IP address.
Current Status	Indicates the status of a manual power adjustment request.
AP MAC Address	The managed AP Ethernet MAC address.
Location	A descriptive location string configured for the managed AP.
Radio	The radio interface on the managed AP.
Current Power	The current transmit power on the managed AP radio.
New Power	The new transmit power computed by the power algorithm.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless power-plan proposed
Switch IP Address  Current Status
-----------------  ---------------
10.0.0.1           Algorithm Completed
10.254.22.1        Algorithm Completed
10.254.22.15       Algorithm Completed


(DWS-4026) #show wireless power-plan proposed 10.254.22.15
Current Status.............................. Algorithm Complete
No proposed power adjustments to display.
```

PEER UNIFIED SWITCH COMMANDS

The commands in this section provide peer Unified Switch status.

show wireless peer-switch

This command displays status information for peer Unified Switches. If no parameters are entered, the command will display summary status for all peer switches. If a peer switch IP address is entered, detailed status for that peer switch is displayed.

Format **show wireless peer-switch** *[<ipaddr>]*

Mode Privileged EXEC

Field	*Description*
ipaddr	The *<ipaddr>* is a valid IP address.
IP Address	IP address of the peer switch.
Vendor ID	The peer switch software vendor ID.
Software Version	Version of WS software on the peer switch.
Protocol Version	Protocol version of WS software on the peer switch.
Discovery Reason	Method for peer WS discovery.
Managed AP Count	Total number of access points currently managed by the peer switch.
Age	Time since last update was received from the switch.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless peer-switch

                 Vendor   Software              Protocol  Discovery
IP Address       ID       Version               Version   Reason     Age
---------------  ------   --------------------  --------  ---------  -----------
10.27.64.222     D-Link   D.5.28.1              2         L2 Poll    0d:00:00:18

(DWS-4026) #show wireless peer-switch 10.254.22.1

IP Address..................................... 10.254.22.1
Vendor ID...................................... D-Link
Software Version............................... D.5.28.1
Protocol Version............................... 2
Discovery Reason............................... L2 Poll
Managed AP Count............................... 3
Age............................................ 0d:00:00:11
```

show wireless peer-switch configure status

This command displays config push status information for peer Unified Switches. If no parameters are entered, the command will display summary status for all peer switches. If a peer switch IP address is entered, detailed status for that peer switch is displayed.

Format **show wireless peer-switch** *[<ipaddr>]* **configure status**

Mode Privileged EXEC

Field	*Description*
ipaddr	The *<ipaddr>* is a valid IP address.
IP Address	The IP address of the peer switch.
Configuration Switch IP Address	The peer switch IP address last config received.
Configuration Status	Config push status from the Unified Switch to this peer switch.
Configuration Received	Configuration groups received as part of config push from the peer switch.
Rx Time	The time the config push was received from the peer switch.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless peer-switch configure status
                Configuration
IP Address      Switch IP Address   Configuration               Rx Time
--------------  ------  -------------------  --------  ---------  -----------
10.0.0.100      10.254.22.1        AP Database,AP Profile..  JAN 03 23:32:06 1970
10.0.0.101      10.254.22.1        AP Database,AP Profile..  JAN 03 23:32:06 1970
10.0.0.102      10.254.22.1        AP Profile,Channel..      JAN 03 23:32:06 1970

(DWS-4026) #show wireless peer-switch 10.0.0.100 configure status

IP Address..................................... 10.0.0.100
Configuration Switch IP Address.    ... .....  10.254.22.1
Configuration Status  ......................... Failure Invalid Code Version
Configuration Received......................... AP Database,
                                                AP Profile,
                                                Channel Power,
                                                Discovery,
                                                Global,
                      Known-Client
Rx Time   ..................                      JAN 03 23:32:06 1970
```

show wireless peer-switch ap status

This command displays the operational status for a peer Unified Switch-managed AP. If no parameters are specified, the command will display a summary of all Unified Switch-managed APs. If an AP MAC address is specified, the detailed status is displayed.

Format **show wireless peer-switch** *[<ipaddr>]* **ap** *[<macaddr>]* **status**

Mode Privileged EXEC

Field	*Description*
ipaddr	The *<ipaddr>* is a valid IP address.

Field	*Description*
macaddr	Unified Switch-managed AP MAC address.
IP Address	The network IP address of the peer Unified Switch-managed AP.
MAC Address	The Ethernet address of the peer Unified Switch-managed AP.
Peer Switch IP Address	The network IP address of the peer Unified Switch managing the AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Profile	The AP profile configuration currently applied to the peer Unified Switch-managed AP.
Hardware Type	Hardware platform for the AP, this is learned from the AP during discovery.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless peer-switch ap status
                   Peer Switch
MAC Address        IP Address         Location       Profile        HwType
-----------------  ---------------    ------------   -------------  -----------
00:01:01:02:01:01  192.168.0.100      Ground Floor   1-Default      DWL-8600AP Dual Radio a/b/g/n
00:01:01:02:02:01  192.168.0.100      Ground Floor   1-Default      DWL-8600AP Dual Radio a/b/g/n
00:01:01:02:03:0   192.168.0.200      Conf Room…     2-L3 Roaming.. DWL-8600AP Dual Radio a/b/g/n
00:01:01:02:04:01  192.168.0.300      First Floor    3-WPA2 VAPs..  DWL-8600AP Dual Radio a/b/g/n

(DWS-4026) #
(DWS-4026) #show wireless peer-switch 192.168.0.100 ap status
                   Peer Switch
MAC Address        IP Address     Location       Profile        HwType
-----------------  -------------- ------------   -------------  -----------
00:01:01:02:01:01  192.168.0.100  Ground Floor   1-Default      DWL-8600AP Dual Radio a/b/g/n
00:01:01:02:02:01  192.168.0.100  Ground Floor   1-Default      DWL-8600AP Dual Radio a/b/g/n


(DWS-4026) #show wireless peer-switch ap 00:01:01:02:02:01 status

MAC Address..................................... 00:01:01:02:01:01
Peer Switch IP Address. .......................192.168.0.100
IP Address.   ................................. 192.168.0.1
Location........................................ Conf Room Bldg 200
Profile......................................... 2 - L3 Roaming Profile
Hardware Type................................... D-Link
```


LOCAL ACCESS POINT DATABASE COMMANDS

The commands in this section provide configuration of the local valid AP database. These configurations may also be performed on an external RADIUS server.

ap database

This command adds an AP to the local valid AP database (if not already present) and enters the AP configuration mode identified by the AP MAC address. In AP configuration mode, you can configure parameters for each individual valid AP. Note that if a valid AP is already being managed by the switch, you need to reset the AP to pick up any configuration changes in the valid AP database. The valid AP database parameters are read only when the AP is validated during discovery.

Format **ap database** *<macaddr>*
Mode Wireless Config

Parameter	*Description*
macaddr	MAC address of a physical AP.

no ap database

The **no** version of this command deletes the AP entry for the specified MAC address from the local database or all the entries present in the database.

Format **no ap database** *[<macaddr>]*
Mode Wireless Config

mode (AP Config Mode)

This command configures the managed mode for an AP.

Default ws-managed
Format **mode** *{ws-managed | standalone | rogue}*
Mode AP Config

Parameter	*Description*
ws-managed	AP is managed by the Unified Switch upon discovery.
standalone	AP is managed as a standalone AP and should not be reported as rogue by the Unified Switch.
rogue	AP is identified as an administrator-configured rogue AP and will be reported as rogue upon discovery.

location

This command configures a descriptive string for the AP location.

Format	**location** *<value>*
Mode	AP Config

Parameter	*Description*
value	This parameter is an AP location string. It should not be more than 32 characters long. To use spaces in the location, enclose the value with quotes, for example "Conference Room A".

no location

The **no** version of this command deletes the current location string for the AP.

Format	**no location**
Mode	AP Config

password (AP Config Mode)

This command configures the password that this AP must use to authenticate to the Unified Switch. The password is only verified if global AP authentication is enabled. After you enter the password, the CLI prompts you to enter a password that is between 8-63 alphanumeric characters.

Default	The default password is blank.
Format	**password**
Mode	AP Config

no password

The **no** version of this command deletes the password for the AP.

Format	**no password**
Mode	AP Config

Example: The following shows an example of the command.

```
DWS-4026 (Config-ap)# password ?
<cr>Press Enter to execute the command.

DWS-4026 (Config-ap)# password <cr>
Enter Password (8 - 63 characters):<enter here>
Re-enter password:<enter same here>

DWS-4026 (Config-ap)# no password <cr>
DWS-4026 (Config-ap)#
```

password encrypted

This command configures the password that this AP must use to authenticate to the Unified Switch. The password is only verified if global AP authentication is enabled. The command accepts the AP password in an encrypted format.

Default The default password is blank.

Format **password encrypted** *<password>*

Mode AP Config

Parameter	*Description*
password	The password in encrypted format, 128 hexadecimal characters.

profile

This command configures the AP profile to be used to configure this AP. The profile configuration is used only if the AP mode is Unified Switch-managed.

Default 1 - Default

Format **profile** *<1-16>*

Mode AP Config

Parameter	*Description*
1-16	Indicates the AP profile ID for AP configuration.

no profile

The **no** version of this command sets the current profile ID for the AP to the default profile.

Format **no profile**

Mode AP Config

radio

This command allows you to configure fixed channel and/or power settings for a radio on the AP. If the channel is not valid for the physical mode configured within the AP configuration profile, this configuration is ignored.

Default channel 0 (auto), power 0 (auto)

Format **radio** *<1-2> {channel <channel> | power <0-100>}*

Mode AP Config

Parameter	*Description*
1-2	The radio interface on the AP.
channel	0 (auto) or a fixed channel for the radio. The valid range is based on the configured country code.
0-100	0 (auto) or a fixed transmit power for the radio. The value is entered as % of maximum power.

standalone channel (Stand-alone AP expected channel)

This command configures the expected channel for an AP in stand-alone mode.

Default 0 (any channel)

Format **standalone channel** *<channel>*

Mode AP Config

Parameter	*Description*
channel	A valid channel from 0 to 161 from the all-country aggregate channel list. Channel zero indicates that any valid channel is allowed.

no standalone channel

The **no** version of this command configures the expected channel for an AP in stand-alone mode to the default – any channel is allowed.

Format `no standalone channel`

Mode AP Config

standalone security (Stand-alone AP expected security mode)

This command configures the expected security mode for an AP in stand-alone mode.

Default any

Format **standalone security** *{any | open | wep | wpa}*

Mode AP Config

Parameter	*Description*
any	All security modes are allowed; open security, WEP and WPA/WPA2.
open	Only open security mode is allowed for the AP.
wep	Only WEP security is allowed for the AP.
wpa	Only WPA/WPA2 security is allowed for the AP.

no standalone security

The **no** version of this command configures the expected security mode for an AP in stand-alone mode to the default – any security mode is allowed.

Format **no standalone security**

Mode AP Config

standalone ssid (Stand-alone AP expected SSID)

This command configures the expected SSID for an AP in stand-alone mode.

Default " " (empty string – any SSID is allowed).

Format **standalone ssid** *<name>*

Mode AP Config

Parameter	*Description*
name	The service set ID must be between 1 and 32 characters. Use the **no** form of the command to configure the AP to operate on any SSID.

no standalone ssid

The **no** version of this command configures the expected SSID for an AP in stand-alone mode.

Format **no standalone ssid**

Mode AP Config

standalone wds-mode (Stand-alone AP expected WDS mode)

This command configures the expected WDS mode for an AP in stand-alone mode.

Default any

Format **standalone wds-mode** *{any | bridge | normal}*

Mode AP Config

Parameter	*Description*
any	Operation as a bridge or in normal mode is allowed.
bridge	Normal mode operation is not allowed. The stand-alone AP is expected to operate as a bridge.
normal	Operation as a bridge is not allowed.

no standalone wds-mode

The **no** version of this command configures the expected WDS mode for an AP in stand-alone mode to the default – any WDS mode is allowed.

show wireless ap database

This command displays the valid AP database entries. If no parameters are entered, a summary is displayed. You can enter a MAC address to display detailed information for a specific AP.

Format **show wireless ap database** *[<macaddr>]*

Mode Privileged EXEC

Field	*Description*
macaddr	The MAC Address corresponding to the AP's Ethernet interface.

Field	*Description*
Location	A description for the AP, often based on its location.
AP Mode	Indicates the configured mode of the AP is either `ws-managed`, `standalone`, or `rogue`.
Profile	This indicates the configuration profile. If the AP is in managed mode this is the profile sent to the AP.
Password Configured	If the authentication password is configured, the value displayed will be *Yes*, otherwise it will be *No*.
Radio 1 Channel	This indicates Auto or a fixed channel for radio 1.
Radio 2 Channel	This indicates Auto or a fixed channel for radio 2.
Radio 1 Transmit Power	This indicates Auto or a fixed power setting for radio 1.
Radio 2 Transmit Power	This indicates Auto or a fixed power setting for radio 2.
Standalone Expected Channel	Expected channel for stand-alone mode.
Standalone Expected Security Mode	Expected security for stand-alone mode.
Standalone Expected SSID	Expected SSID for stand-alone mode.
Standalone Expected WDS Mode	Expected WDS mode for stand-alone mode.

When the command is entered without specifying a MAC address, the following summary information displays:

Field	*Description*
AP Database	Number of APs in the database/size of the AP database.
Managed AP	The total number of APs in the database that are marked as Managed.
Rogue AP	The total number of APs in the database that are marked as Rogue.
Standalone AP	The total number of APs in the database that are marked as Standalone.

Example: The following example shows the CLI display when the command is enter with no AP MAC address specified:

```
AP database: 2/128    Managed AP: 1     Rogue AP: 0    Standalone AP: 1

MAC Address           Location                          AP Mode
--------------------  --------------------------------  -------------
00:11:22:33:45:67     test                              ws-managed
00:23:34:56:54:76     dev                               standalone
```

Example: The following shows example CLI display output for the command when an AP MAC address is specified..

```
(DWS-4026) #show wireless ap database 11:33:44:55:66:77

AP MAC Address................................ 11:33:44:55:66:77
Location.....................................
AP Mode....................................... ws-managed
Password Configured........................... No
Profile....................................... 1 - Default
```



```
Radio  1 Channel.............................. Auto
Radio  1 Power................................ Auto
Radio  2 Channel.............................. Auto
Radio  2 Power................................ Auto
Stand-alone Expected Channel.................. 0
Stand-alone Expected Security Mode............ Any
Stand-alone Expected SSID.....................
Stand-alone Expected WDS Mode................. Any

(DWS-4026) #show wireless ap-database
MAC Address           Location                          AP Mode
--------------------  --------------------------------  -------------
00:77:77:77:52:00     lab                               ws-managed
11:10:10:10:10:10     conference-room                   standalone
```

WIRELESS NETWORK COMMANDS

The commands in this section provide configuration of wireless networks.

network (Wireless Config Mode)

This command adds a network configuration (if not already present) and enters the network configuration mode. In this mode, you can modify the network configuration parameters.

Default	Networks 1-16 are created by default.
Format	**network** *<1-64>*
Mode	Wireless Config

Parameter	*Description*
1-64	Integer ID for the network.

no network

The **no** version of this command deletes a configured network. 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	**no network**
Mode	Wireless Config

ssid

This command configures 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.

Default	Network 1 - Guest Network Network *<networkid>* – Managed SSID *<networkid>*
Format	**ssid** *<name>*
Mode	Network Config

Parameter	*Description*
name	Service Set Identifier, must be between 1-32 alphanumeric characters. To use spaces in the SSID, use quotes around the name.

vlan (Network Config Mode)

This command configures the default VLAN ID for the network. If there is no RADIUS server configured or a client is not associated with a VLAN via RADIUS, this is the VLAN assigned.

Default 1 – Default VLAN
Format **vlan** *<1-4094>*
Mode Network Config

Parameter	*Description*
1-4094	A valid VLAN ID.

no vlan

The **no** version of this command sets the default VLAN ID for the network to its default value.

Format **no vlan**
Mode Network Config

hide-ssid

This command enables hiding of the SSID for this network. If enabled, the SSID is not included in the AP beacon frames.

Default Disable
Format **hide-ssid**
Mode Network Config

no hide-ssid

The **no** version of this command disables hiding of the SSID for this network.

Format **no hide-ssid**
Mode Network Config

client-qos access-control

This command configures the default access control list used by clients associated with this network that do not obtain their own value via RADIUS. The *<acl-name>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters. The access list specified in this command must currently exist in the Unified Switch.

Format **client-qos access-control** *{down | up} {ip {<1-199> | <acl-name>}*
Mode Network Config

no client-qos access-control

The **no** version of this command removes the client QoS default access control list parameter configured for this network.

Format **no client-qos access-control** *{down | up}*
Mode Network Config

client-qos bandwidth-limit

This command configures 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.

Note: The specified value is subject to rounding down to the nearest 64000 in the AP, with a minimum rounded value of 64000.

Format **client-qos bandwidth-limit** *{down | up} {1-4294967295}*
Mode Network Config

no client-qos bandwidth-limit

The **no** version of this command sets the client QoS default maximum bandwidth rate limit parameter to 0 for this network, disabling rate limiting for clients that associate with this network and use this default value.

Format **no client-qos bandwidth-limit** *{down | up}*
Mode Network Config

client-qos diffserv-policy

This command configures the default Diffserv policy used by clients associated with this network that do not obtain their own value via RADIUS. The *<policy-name>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters and must specify a Diffserv policy that currently exists in the Unified Switch.

Format **client-qos diffserv-policy** *{down | up} <policy-name>*
Mode Network Config

no client-qos diffserv-policy

The **no** version of this command removes the client QoS default Diffserv policy parameter configured for this network.

Format **no client-qos diffserv-policy** *{down | up}*
Mode Network Config

client-qos enable

This command enables AP client QoS operation for the network. When enabled, and when the wireless global client QoS mode is also 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).

Note: This command takes effect in an AP without requiring that the AP profile be reapplied.

Default disable
Format **client-qos enable**
Mode Network Config

no client-qos enable

The **no** version of this command disables AP client QoS operation for the network. Client traffic is not subject to QoS processing for any clients attached to this wireless network.

Format	**no client-qos enable**
Mode	Network Config

deny-broadcast

This command enables deny broadcast mode for the network. This means the AP will not respond to client probe requests broadcast to all available SSIDs.

Default	Disable
Format	**deny-broadcast**
Mode	Network Config

no deny-broadcast

The **no** version of this command disables deny broadcast mode for the network. This means the AP will respond to client probe requests for all available SSIDs.

Format	**no deny-broadcast**
Mode	Network Config

redirect mode

This command enables and configures the mode for redirection of wireless client traffic on this network. If HTTP redirection is enabled, initial client requests are redirected to the configured URL.

Default	None
Format	**redirect mode** *{http | none}*
Mode	Network Config

no redirect mode

The **no** version of this command disables redirect on the network.

Format	**no redirect mode**
Mode	Network Config

redirect url

This command configures a URL for HTTP redirection. When HTTP redirection is enabled on the network, each initial client request is directed to this URL. Note that http:// is not entered in the configured URL because this prefix is assumed.

Default	None (The default is “blank”.)
Format	**redirect url** *<url>*
Mode	Network Config

Parameter	*Description*
url	A Uniform Resource Locator, for example www.cnn.com. The URL must be 0-128 characters.

no redirect url

The **no** version of this command removes the configured URL. The value is set to an empty string.

Format	**no redirect** url
Mode	Network Config

security mode

This command configures the authentication and encryption mode on the network.

Default	none
Format	**security mode** *{none	static-wep	wep-dot1x	wpa-enterprise	wpa-personal}*
Mode	Network Config

Parameter	*Description*
none	No authentication or encryption on the network.
static-wep	Static WEP encryption, authentication is configured separately.
wep-dot1x	Dynamic WEP authentication using 802.1x.
wpa-enterprise	WPA 802.1x authentication.
wpa-personal	WPA shared-key authentication.

no security mode

The **no** version of this command sets the security mode to its default value.

Format	**no security mode**
Mode	Network Config

wep authentication

This command configures the static WEP authentication mode for the network. This value is applicable only when the security mode is configured for static WEP authentication and encryption.

Default Open System

Format **wep authentication** *{open-system [shared-key] | shared-key}*

Mode Network Config

Parameter	*Description*
open system	No authentication required.
shared-key	Clients are required to authenticate to the network using a shared key.

no wep authentication

The **no** version of this command sets WEP authentication mode to the default value, which is **open system**.

Format **no wep authentication**

Mode Network Config

wep key

This command configures 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.

Format **wep key** *<1-4> <value>*

Mode Network Config

Parameter	*Description*
1-4	A valid WEP key index.
value	The WEP key itself, entered in ASCII or HEX format. The following list shows the number of keys to enter in the field: • 64 bit —ASCII: 5 characters; Hex: 10 characters • 128 bit —ASCII: 13 characters; Hex: 26 characters • 152 bit —ASCII: 16 characters; Hex: 32 characters. For more information, please see the “Static WEP” table in the *Unified Switch Administrator’s Guide*.

no wep key

The **no** version of this command removes the corresponding WEP key configuration.

Format **no wep key** *<1-4>*

Mode Network Config

wep tx-key

This command configures the WEP key index to be used for encryption on the network. This value is applicable only when the security mode is configured for WEP shared key authentication and encryption.

Default 1
Format **wep tx-key** *<1-4>*
Mode Network Config

Parameter	*Description*
1-4	A valid WEP key index value.

no wep tx-key

The **no** version of this command sets the WEP transmit key index to its default value.

Format **no wep tx-key**
Mode Network Config

wep key type

This command configures the WEP key type for the network. The configured key type is used when the network security mode is set to WEP shared key. The WEP key type affects the number of characters required for a valid WEP key, and therefore changing the WEP key length will reset all keys.

Default ASCII
Format **wep key type** *{ascii | hex}*
Mode Network Config

Parameter	*Description*
ascii	Set WEP key type to ASCII.
hex	Set WEP key type to hexadecimal.

no wep key type

The **no** version of this command returns the WEP key type to its default value.

Format **no wep key type**
Mode Network Config

wep key length

This command configures the WEP key length in bits for the network. The configured key length is used when the network security mode is set to WEP shared key. The WEP key length affects the number of characters required for a valid WEP key, and therefore changing the WEP key length will reset all keys.

Default 128
Format **wep key length** *{64 | 128}*
Mode Network Config

no wep key length

The **no** version of this command returns the WEP key length to its default value.

Format	**no wep key length**
Mode	Network Config

mac authentication

This command enables and configures the mode for client MAC authentication on the network.

Default	Disable
Format	**mac authentication** *{local | radius}*
Mode	Network Config

Parameter	*Description*
local	Enable MAC authentication using the AP profile MAC authentication list.
radius	Enable MAC authentication using the configured RADIUS server.

no mac authentication

The **no** version of this command disables MAC authentication on the network.

Format	**no mac authentication**
Mode	Network Config

radius server secret (Network Config)

This command configures the secret to use in communicating with the configured RADIUS server. The secret must be a printable string in the range 0-64 characters. When the command is entered, you will be prompted to enter the secret and then again to confirm the secret.

Format	**radius server secret**
Mode	Network Config

Example: The following shows an example of the command.

```
DWS-4026 (Config-network)# radius server secret
Enter Secret (65 characters max):<enter here>
Re-enter Secret:<enter same here>
```

radius server-name

This command configures the RADIUS authentication/accounting server name for wireless clients authenticating to this network. The server name can contain alphanumeric characters plus –, _, and space.

Default	Default-RADIUS-Server – authentication server name Default-RADIUS-Server – accounting server name
Format	**radius server-name** *{auth | acct} <name>*
Mode	Network Config

Parameter	*Description*
name	Enter an alphanumeric string up to 32 characters in length.

no radius server-name

The **no** version of this command sets the RADIUS authentication/accounting server name to the default value.

Format	**no radius server-name** *{auth | acct}*
Mode	Network Config

Example: The following shows an example of the command.

```
(DWS-4026) #radius server-name auth  "Wireless_Network-1 Auth_Server 1" ?
<cr>   Press Enter to execute the command.

(DWS-4026) #no radius server-name auth ?
<cr>   Press Enter to execute the command.

(DWS-4026) #radius server-name acct  "Wireless_Network-1 Acct_Server 1" ?
<cr>   Press Enter to execute the command.

(DWS-4026) #no radius server-name acct  ?
<cr>   Press Enter to execute the command.
```

radius use–network–configuration

This command configures the system to use the network RADIUS configuration for wireless client's authentication on this network or to use global RADIUS configuration.

Default	Enable
Format	**radius use-network-configuration**
Mode	Network Config

no radius use–network–configuration

The **no** version of this command configures the system to use the network RADIUS configuration for authentication of wireless clients on this network.

Format	**no radius use-network-configuration**
Mode	Network Config

Example: The following shows an example of the command.

```
(DWS-4026) # radius use-network-configuration ?
```



```
<cr>Press Enter to execute the command.

(DWS-4026) # no radius use-network-configuration ?
<cr>Press Enter to execute the command.
```

radius accounting (Network Config)

This command enables RADIUS accounting mode for authentication on this network.

Default	Disable
Format	**radius accounting**
Mode	Network Config

no radius accounting

The **no** version of this command disables RADIUS accounting mode for authentication on this network.

Format	**no radius accounting**
Mode	Network Config

wpa versions

This command configures the WPA version(s) supported on the network. One or both parameters must be specified. This configuration only applies when the configured security mode is **WPA**.

Default	wpa/wpa2
Format	**wpa versions** *{wpa [wpa2] | wpa2}*
Mode	Network Config

Parameter	*Description*
wpa	WPA version allowed.
wpa2	WPA2 version allowed.

no wpa versions

The **no** version of this command configures the supported WPA versions to the default value.

Format	**no wpa versions**
Mode	Network Config

wpa ciphers

This command configures the WPA cipher suites supported on the network; one or both parameters must be specified. This configuration only applies when the configured security mode is **WPA**.

Default	tkip
Format	**wpa ciphers** *{ccmp [tkip] | tkip}*
Mode	Network Config

Parameter	*Description*
tkip	TKIP encryption.
ccmp	CCMP encryption.

no wpa ciphers

The **no** version of this command WPA returns supported cipher suites to the default value.

Format	**no wpa ciphers**
Mode	Network Config

wpa key

This command configures 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 to WPA shared key.

Default	None
Format	**wpa key** *<value>*
Mode	Network Config

tunnel

This command enables client traffic tunneling on the network. For the tunnel to be operational, global routing must be enabled on the switch and the tunnel subnet, and mask must be configured and match a valid routing interface.

Default	Disable
Format	**tunnel**
Mode	Network Config

no tunnel

The **no** version of this command disables client traffic tunneling on the network.

Format	**no tunnel**
Mode	Network Config

tunnel subnet

This command configures the tunnel subnet IP address for the network. This must match a configured routing interface in order for the tunnel to be operational.

Default	Subnet IP - None Subnet mask - 255.255.255.0
Format	**tunnel subnet** *<ipaddr> [mask <mask>]*
Mode	Network Config

Parameter	*Description*
ipaddr	A valid IP address.
mask	A valid subnet mask.

no tunnel subnet

The **no** version of this command deletes the configured tunnel subnet parameters.

Format	**no tunnel subnet**
Mode	Network Config

arp-suppression

This command enables wireless ARP suppression on the network. Enabling wireless ARP suppression allows for limiting ARP broadcasts on the wireless medium for IPv4 networks.

Default	Disable
Format	**arp-suppression**
Mode	Network Config Mode

no arp-suppression

The **no** version of this command disables wireless ARP suppression on the network.

Format	**no arp-suppression**
Mode	Network Config Mode

wpa2 pre-authentication

This command enables WPA2 pre-authentication support for client roaming.

Default	Enable
Format	**wpa2 pre-authentication**
Mode	Network Config

no wpa2 pre-authentication

The **no** version of this command disables WPA2 pre-authentication support.

Format `no wpa2 pre-authentication`
Mode Network Config

wpa2 pre-authentication limit

This command configures 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.

Default 0, no limit
Format `wpa2 pre-authentication limit <0-192>`
Mode Network Config

Parameter	*Description*
0-192	Valid WPA2 pre-authentication limit.

no wpa2 pre-authentication limit

The **no** version of this command sets the configured WPA2 pre-authentication limit to its default value.

Format `no wpa2 pre-authentication limit`
Mode Network Config

wpa2 key-forwarding

This command enables WPA2 key forwarding support for client roaming on the network.

Default Enable
Format `wpa2 key-forwarding`
Mode Network Config

no wpa2 key-forwarding

The **no** version of this command disables WPA2 key forwarding support on the network.

Format `no wpa2 key-forwarding`
Mode Network Config

wpa2 key-caching holdtime

This command configures the length of time a PMK will be cached by an AP for either client roaming or key forwarding.

Default 10
Format `wpa2 key-caching holdtime <0-1440>`
Mode Network Config

Parameter	*Description*
0-1440	WPA2 key caching hold time in minutes.

no wpa2 key-caching holdtime

The **no** version of this command sets the WPA2 key caching hold time to its default value.

Format **no wpa2 key-caching holdtime**
Mode Network Config

dot1x bcast-key-refresh-rate

This command specifies the interval after which the broadcast keys are changed.

Default 300 seconds
Format **dot1x bcast-key-refresh-rate** *<0-86400>*
Mode Network Config

Parameter	*Description*
0-86400	The bcast-key-refresh-rate range is 0 to 86400 in seconds.

no dot1x bcast-key-refresh-rate

The **no** version of this command returns the bcast-key-refresh-rate to its default value.

Format **no dot1x bcast-key-refresh-rate**
Mode Network Config

dot1x session-key-refresh-rate

This command specifies the interval after which the Unicast session keys are changed.

Default 0 seconds
Format **dot1x session-key-refresh-rate** *<0-86400>*
Mode Network Config

Parameter	*Description*
0-86400	The session-key-refresh-rate range is 0 to 86400 in seconds.

no dot1x session-key-refresh-rate

The **no** version of this command returns the session-key-refresh-rate to its default value.

Format `no dot1x session-key-refresh-rate`
Mode Network Config

clear (Network Config Mode)

This command restores a network configuration to default values.

Format `clear`
Mode Network Config

show wireless network

This command displays the network configuration parameters. If no parameters are specified, a summary of the configured networks is displayed, otherwise the detailed configuration is displayed.

Format `show wireless network` *[<1-64>]*
Mode Privileged EXEC

Field	*Description*
SSID	Service Set Identifier.
Interface ID	Internal interface number for this network
Default VLAN	Default VLAN for the network.
Hide SSID	Indicates if SSID inclusion is suppressed from the beacons.
Deny Broadcast	Indicates if probe requests with broadcast SSID are denied on the network.
Redirect Mode	Indicates the mode of client traffic redirection.
Redirect URL	Indicates the configured URL for client HTTP redirection.
L2 Distributed Tunneling Mode	Indicates whether L2 distributed tunneling mode is enabled on the switch.
Bcast Key Refresh Rate	The interval after which the broadcast keys are changed.
Session Key Refresh Rate	the interval after which the Unicast session keys are changed
L3 Tunnel Mode	If tunneling feature is enabled, indicates if L3 roaming is enabled on the network.
L3 Tunnel Status	Indicates the if the tunnel is up or down.
L3 Tunnel Subnet IP	If tunneling feature is enabled, indicates the subnet for the tunnel.
L3 Tunnel Subnet Mask	If tunneling feature is enabled, indicates the network mask for the tunnel subnet.
Wireless ARP Suppression	Indicates whether wireless ARP suppression is enabled or disabled.
Security Mode	Indicates the authentication and encryption mode.
MAC Authentication	The client MAC address authentication mode.
RADIUS Authentication Server Name	RADIUS server name for authentication.
RADIUS Authentication Server Status	Indicates whether the specified named RADIUS Authentication server is configured in the RADIUS Client configuration.
RADIUS Accounting Server Name	RADIUS server name for accounting.
RADIUS Accounting Server Status	Indicates whether the specified named RADIUS Accounting server is configured in the RADIUS Client configuration.

Field	*Description*
WPA Versions	Indicates the WPA versions allowed when the WPA encryption mode is enabled.
WPA Ciphers	Indicates the encryption solutions to use when the WPA encryption mode is enabled.
WPA Key Type	Specifies the type of the WPA key configured (ASCII only).
Passphrase	The WPA passphrase
WPA2 Pre-Authentication	If WPA2 version is enabled, indicates pre-authentication support for roaming WPA2 clients.
WPA2 Pre-Authentication Limit	If WPA2 pre-authentication is enabled, specifies a limit on the number of APs within the peer group to which one client is allowed to pre-authenticate.
WPA2 Key Caching Holdtime	Time in minutes that a PMK will be cached by an AP after the client using this PMK has roamed away from this AP.
WEP Authentication Type	Indicates whether Open System authentication or Shared Key authentication is used.
WEP Key Type	indicates whether the key is in hexadecimal format or ASCII text format.
WEP Key Length	If WEP – Shared Key security mode is enabled, specifies number of bits for the WEP Keys.
WEP Transfer Key Index	If WEP – Shared Key security mode is enabled, indicates which WEP key will be used for encryption.
WEP Key1-4	If WEP – Shared Key security mode is enabled, indicates the WEP keys configured for encryption. Up to 4 keys can be configured.
Client QoS Mode	Indicates whether client QoS operation is enabled on this network.
Client QoS Bandwidth Limit Down	Defines 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.
Client QoS Bandwidth Limit Up	Defines 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.
Client QoS Access Control Down	Defines 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.
Client QoS Access Control Up	Defines 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.
Client QoS Diffserv Policy Down	Defines 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.
Client QoS Diffserv Policy Up	Defines 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.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless network

Network  SSID                              Hide SSID  L3 Tunnel   Security Mode
-------  --------------------------------  ---------  ----------  -------------
1        dlink1                            Disable    Disable     None
2        dlink2                            Disable    Disable     None
3        dlink3                            Disable    Disable     None
4        dlink4                            Disable    Disable     None
5        dlink5                            Disable    Disable     None
6        dlink6                            Disable    Disable     None
7        dlink7                            Disable    Disable     None
```

```
8       dlink8                              Disable    Disable     None
9       dlink9                              Disable    Disable     None
10      dlink10                             Disable    Disable     None
11      dlink11                             Disable    Disable     None
12      dlink12                             Disable    Disable     None
13      dlink13                             Disable    Disable     None
14      dlink14                             Disable    Disable     None
15      dlink15                             Disable    Disable     None
16      dlink16                             Disable    Disable     None

(DWS-4026) #show wireless network 3

SSID..................................... dlink3
Interface ID............................. 264
Default VLAN............................. 1
Hide SSID................................ Disable
Deny Broadcast........................... Disable
Redirect Mode............................ None
Redirect URL............................. -----
L2 Distributed Tunneling Mode............ Disable
Bcast Key Refresh Rate................... 300
Session Key Refresh Rate................. 0
L3 Tunnel Mode........................... Disable
L3 Tunnel Status......................... None
L3 Tunnel Subnet IP...................... 0.0.0.0
L3 Tunnel Subnet Mask.................... 255.255.255.0
Wireless ARP Suppression................. Disable
Security Mode............................ None
MAC Authentication....................... Disable
RADIUS Authentication Server Name........ Default-RADIUS-Server
RADIUS Authentication Server Status...... Not Configured
RADIUS Accounting Server Name............ Default-RADIUS-Server
RADIUS Accounting Server Status.......... Not Configured
WPA Versions............................. WPA/WPA2
WPA Ciphers.............................. TKIP/CCMP
WPA Key Type............................. ASCII
Passphrase.............................
WPA2 Pre-Authentication.................. Enable
WPA2 Pre-Authentication Limit............ 0
WPA2 Key Caching Holdtime (minutes)...... 10
WEP Authentication Type.................. Open System
WEP Key Type............................. HEX
WEP Key Length (bits).................... 128
WEP Transfer Key Index................... 1
WEP Key 1.............................
WEP Key 2.............................
WEP Key 3.............................
WEP Key 4.............................
Client QoS Mode.......................... Disable
Client QoS Bandwidth Limit Down.......... 0
Client QoS Bandwidth Limit Up............ 0
Client QoS Access Control Down........... -----
Client QoS Access Control Up............. -----
Client QoS Diffserv Policy Down.......... -----
--More-- or (q)uit
Client QoS Diffserv Policy Up............ -----
```


ACCESS POINT PROFILE COMMANDS

The commands in this section provide configuration of access point profiles. Access point profiles can be applied to multiple physical APs.

ap profile

This command adds an AP profile (if not already present) and enters the AP profile configuration mode. In this mode, you can modify the profile configuration parameters. You can modify an AP profile at any time. If the profile is associated with one or more Managed APs, you must use the `wireless ap profile apply` command to send the changes to those APs.

Default 1 - Default

Format **`ap profile`** *<1-16>*

Mode Wireless Config

Parameter	*Description*
1-16	Identifier for the AP Profile.

no ap profile

The **`no`** version of this command deletes a configured 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 **`no ap profile`** *<1-16>*

Mode Wireless Config

Example: The following shows an example of the command.

```
DWS-4026 (Config-wireless)# ap profile 1
DWS-4026 (Config-ap-profile)#
```

If the profile is in use:

```
DWS-4026 (Config-wireless)# no ap profile 2
One or more managed APs are configured with this profile, it cannot be deleted.
```

name

This command allows you to configure a descriptive name for the AP Profile.

Default Default (AP profile 1)

Format **`name`** *<name>*

Mode AP Profile Config

Parameter	Description
name	AP Profile name; it must be less than 32 characters. Use quotes around a name that contains spaces.

no name

The **no** version of this command deletes the configured name for the AP profile.

Format **no name**
Mode AP Profile Config

hwtype

This command allows you to configure the AP hardware type. Currently, only the hw_dwl8600 hardware type is supported.

Default hw_dwl8600
Format **hwtype** *<hw_dwl8600>*
Mode AP Profile Config

Parameter	Description
hw_dwl8600	AP hardware type.

no hwtype

This command allows you to set the AP hardware type to the default value “hw_dwl8600”.

Format **no hwtype**
Mode AP Profile Config

Example: The following shows an example of the command.

```
DWS-4026 (Config-ap-profile)#  no hwtype ?
<cr>   Press Enter to execute the command.
```

vlan (AP Profile Config Mode)

This command allows you to configure the VLAN ID used to send tracer packets by wired network detection algorithm. If VLAN is “0”, the tracer packets will be sent untagged.

Default 1
Format **vlan** *<0-4094>*
Mode AP Profile Config

Parameter	Description
0-4094	Wired network detection VLAN ID.

Example: The following shows an example of the command.

```
DWS-4026 (Config-ap-profile)#  vlan 10 ?
<cr>   Press Enter to execute the command.
```

no vlan (AP Profile Config Mode)

This command allows you to set the wired network detection VLAN ID to the default value. “1”.

Format	**no vlan**
Mode	AP Profile Config

Example: The following shows an example of the command.

```
DWS-4026 (Config-ap-profile)#  no vlan
<cr>   Press Enter to execute the command.
```

ap profile copy

This command copies an entire existing AP profile to another profile. If the destination profile does not exist, it will be created.

Format	**ap profile copy** *<1-16> <1-16>*
Mode	Wireless Config

Parameter	*Description*
1-16	Source AP Profile ID.
1-16	Destination AP Profile ID.

Example: The following shows an example of the command.

If the destination AP Profile is associated with Managed APs:

```
DWS-4026 (Config-wireless)# ap profile copy 1 2 <cr>
The destination profile is associated with WS Managed APs. Do you want to overwrite the
existing profile (y/n)? <enter ‘y’ or ‘n’>
```

wireless ap profile apply

This command requests for the switch 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.

Format	**wireless ap profile apply** *<1-16>*
Mode	Privileged EXEC

Parameter	*Description*
1-16	AP Profile ID.

Example: The following shows an example of the command.

If the profile is associated with WS Managed APs:

```
DWS-4026 (Config-wireless)# ap profile apply 1 <cr>
Do you want to apply the configuration to all managed APs associated with this profile?
(y/n)
```

clear (AP Profile Config Mode)

This command restores an AP profile configuration to default values except for the profile name. The profile name is not an AP configuration and is only used for descriptive purposes, therefore it is not cleared with this command. To delete a profile name, use the **no name** command.

Format	**clear**
Mode	AP Profile Config

Example: The following shows an example of the command.

```
DWS-4026 (Config-ap-profile)# 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
```

show wireless ap profile

This command displays the configured AP profiles. If you do not enter any command parameters, a summary of all AP profiles is displayed. You can enter an AP profile ID to display detailed configuration for a specific profile.

Format	**show wireless ap profile** *[<1-16> [radio [<1-2>]]]*
Mode	Privileged EXEC

Field	*Description*
AP Profile ID	Existing AP profile ID.
Profile Name	A descriptive name for the corresponding AP profile ID.
Hardware Type	Existing AP hardware type ID and description string.
Wired Network Detection VLAN ID	The VLAND ID used for sending tracer packets by the wired network detection algorithm. A configured value of 0 results in the transmission of untagged tracer packets.
Profile Status	Indicates the current AP profile status: • **Configured**—the profile exists, no managed APs are configured with the profile. • **Associated**—one or more managed APs are configured with the profile. • **Apply Requested**—you have invoked the **apply** command for the profile. • **Apply In Progress**—the profile is currently being applied to the associated managed APs. When the **apply** is complete, the profile returns to **Associated** status.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless ap profile 1

AP Profile ID.................................. 1
Profile Name................................... Default
```



```
Hardware Type.............................  0 - Any
Wired Network Detection Vlan ID...........  0 - Any
Profile Status.............................. Configured
Valid APs Configured........................ 0
Managed APs Configured...................... 2
```

ACCESS POINT PROFILE RF COMMANDS

The commands in this section provide RF configuration per radio interface within an access point profile.

radio

This command enters the AP profile radio configuration mode. In this mode you can modify the radio configuration parameters for an AP profile.

Format **radio** *<1-2>*
Mode AP Profile Config

Parameter	*Description*
1-2	The radio interface within the AP profile.

enable (AP Profile Radio Config Mode)

This command configures the administrative mode of the radio interface to the “on” state.

Default on
Format **enable**
Mode AP Profile Radio Config

no enable

The **no** version of this command configures the administrative mode of the radio interface to the “off” state.

Format **no enable**
Mode AP Profile Radio Config

mode (AP Profile Radio Config Mode)

This command configures the physical layer technology to use on the radio.

Default Radio 1, bgn
Radio 2, an
Format **mode** *{a | bg | an | bgn | n-only-a | n-only-g}*
Mode AP Profile Radio Config

Parameter	*Description*
a	Indicates 802.11a as physical mode. Only applicable for radio 1.
bg	Indicates 802.11bg as physical mode. Only applicable for radio 2.
an	Indicates 802.11a/n as physical mode. Only applicable for radio 1.

Parameter	*Description*
bgn	Indicates 802.11b/g/n as physical mode. Only applicable for radio 2.
n-only-a	Indicates 802.11n in 5GHz band as physical mode. Only applicable for radio 1.
n-only-g	Indicates 802.11n in 2.4GHz band as physical mode. Only applicable for radio 2.

If the user attempts to change the radio mode to one that is not applicable to that radio, then the following error displays:

```
(DWS-4026) (Config-ap-profile)#radio 1
(DWS-4026) (Config-ap-radio)#mode bg
Failed to set physical mode for radio interface.
```

no mode (AP Profile Radio Config Mode)

The **no** version of this command is used to return the configured radio mode to the default, which for radio 1 is an and for radio 2 is bgn.

Format **no mode**

Mode AP Profile Radio Config

rf-scan other-channels

This command enables the radio to perform RF scanning on channels other than its operating channel. The optional interval parameter indicates how often the radio leaves its operational channel.

Default
- Enabled
- interval, 60 seconds

Format **rf-scan other-channels** *[interval <30-120>]*

Mode AP Profile Radio Config

Parameter	*Description*
interval	Interval at which the AP will move away from its operating channel.
30-120	Time interval in seconds.

no rf-scan other-channels

The **no** version of this command disables scanning on other channels; the radio will always scan on its operational channel.

Format **no rf-scan other-channels**

Mode AP Profile Radio Config

rf-scan sentry

This command enables dedicated RF scanning and disables normal operation of the radio. The radio will not allow any client associations when sentry mode is enabled.

Default	• Disabled • Channels, all
Format	**rf-scan sentry** *[channels {a | bg | all}]*
Mode	AP Profile Radio Config

Parameter	*Description*
channels	Indicates to scan channels within specified mode/frequency.
a	Perform RF scan on all 802.11a channels (5 GHz frequency).
bg	Perform RF scan on all 802.11b/g channels (2.4 GHz frequency).
all	Perform RF scan on all channels.

no rf-scan sentry

The **no** version of this command disables dedicated scanning and enables normal operation of the radio.

Format	**no rf-scan sentry**
Mode	AP Profile Radio Config

rf-scan duration

This command configures the RF scan duration for the radio. The duration indicates how long the radio will scan on one channel.

Default	10 milliseconds
Format	**rf-scan duration** *<10-2000>*
Mode	AP Profile Radio Config

Parameter	*Description*
10-2000	Time duration in milliseconds.

no rf-scan duration

The **no** version of this command returns the configured RF scan duration to its default value.

Format	**no rf-scan duration**
Mode	AP Profile Radio Config

station-isolation

This command enables 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.

Default Disabled

Format `station-isolation`

Mode AP Profile Radio Config

no station-isolation

The `no` version of this command disables the station isolation mode on the radio.

Format `no station-isolation`

Mode AP Profile Radio Config

rate-limit

This command is used to enable broadcast and multicast traffic rate limiting on the radio. If no optional parameters are entered, the command enables rate limiting on the radio with the default values.

Default
- rate-limit, Disabled
- rate-limit normal, 50 packets per second
- rate-limit burst, 75 packets per second

Format `rate-limit [{normal <1-50> | burst <1-75>}]`

Mode AP Profile Radio Config

Parameter	*Description*
normal	Configures the rate limit for normal traffic; all traffic below this limit is transmitted.
burst	Configures the burst traffic rate. Traffic can occur in bursts up to this value before all traffic is considered to exceed the limit.

no rate-limit

The `no` version of this command is used to either disable broadcast/multicast traffic rate limiting, or to return the configured rate limits to the default values. If no parameters are entered, rate limiting is disabled on the radio. If the optional normal or burst parameters are entered, the specified rate is set to its default value.

Format `no rate-limit [{normal | burst }]`

Mode AP Profile Radio Config

beacon-interval

The command configures the beacon interval for the radio. The beacon interval indicates the interval at which the AP radio transmits beacon frames.

Default 100 milliseconds

Format `beacon-interval <20-2000>`

Mode AP Profile Radio Config

Parameter	Description
20-2000	Time interval in milliseconds at which the radio sends beacon frames.

no beacon-interval

The **no** version of this command configures the beacon interval to the default value.

Format **no beacon-interval**
Mode AP Profile Radio Config

dtim-period

The command configures 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.

Default 10 Beacons
Format **dtim-period** *<1-255>*
Mode AP Profile Radio Config

Parameter	Description
1-255	Number of beacons between DTIMs.

no dtim-period

The **no** version of this command configures the DTIM period to the default value.

Format **no dtim-period**
Mode AP Profile Radio Config

fragmentation-threshold

This command configures 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 there should be no fragmentation.

Default 2346 (no fragmentation)
Format **fragmentation-threshold** *<256-2346>*
Mode AP Profile Radio Config

Parameter	Description
256-2346	Fragmentation threshold for the radio, even values.

no fragmentation-threshold

The **no** version of this command configures the fragmentation threshold to the default value.

Format `no fragmentation-threshold`
Mode AP Profile Radio Config

rts-threshold

This command configures 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.

Default 2347
Format `rts-threshold <0-2347>`
Mode AP Profile Radio Config

Parameter	*Description*
0-2347	RTS threshold for the radio.

no rts-threshold

The **no** version of this command configures the RTS threshold to the default value.

Format `no rts-threshold`
Mode AP Profile Radio Config

max-clients

This command configures the maximum number of simultaneous client associations allowed on the radio interface**.**

Default 200
Format `max-clients <0-200>`
Mode AP Profile Radio Config

Parameter	*Description*
0-200	Maximum number of simultaneous associations allowed on the radio interface.

no max-clients

The **no** version of this command configures the maximum number of simultaneous client associations allowed on the radio interface to the default value.

Format `no max-clients`
Mode AP Profile Radio Config

channel auto

This command enables auto channel adjustment for the radio. This indicates the initial AP channel assignment can be automatically adjusted by the switch.

Default	Disabled
Format	**channel auto**
Mode	AP Profile Radio Config

no channel auto

The **no** version of this command without any parameters disables auto channel adjustment for the radio.

Format	**no channel auto**
Mode	AP Profile Radio Config

channel auto-eligible

This command enables either one or all of the supported channels on the radio to be eligible for auto-channel selection. If you specify one channel, the command will succeed *only if* this channel is supported by the current mode of the radio (use `show wireless ap profile` *XX* `radio` *XX* `auto-eligible` for valid values). If you supply "all" as the argument for this command, all channels supported by the current radio mode will be enabled for automatic selection.

Default	Either all supported channels are enabled, or only channels 1, 6, and 11 if supported by the current radiomode (e.g. 802.11 b/g).
Format	**channel auto-eligible** *{all | <1-255>}*
Mode	AP Profile Radio Config

no channel auto-eligible

The **no** version of this command removes either one or all of the channels currently available for automatic selection from consideration on the radio. If you specify one channel, the command will succeed only if this channel is currently available for automatic selection on the radio. If you supply **all** as the argument for this command, all channels currently available on the radio will be disabled.

Format	**no channel auto-eligible** *{all | <1-255>}*
Mode	AP Profile Radio Config

power auto

This command enables auto power adjustment for the radio. This indicates the AP power assignment can be automatically adjusted by the switch.

Default	Disabled
Format	**power auto**
Mode	AP Profile Radio Config

no power auto

The **no** version of this command disables auto power adjustment for the radio.

Format **no power auto**
Mode AP Profile Radio Config

power default

This command configures a power setting for the radio. When auto power adjustment is enabled, this indicates an initial default power setting; otherwise this indicates a fixed power setting.

Default 100%
Format **power default** *<0-100>*
Mode AP Profile Radio Config

Parameter	*Description*
0-100	Default transmit power percentage.

no power default

The **no** version of this command configures the default power setting to its default value.

Format **no power default**
Mode AP Profile Radio Config

rate

This command is used to configure the list of supported and basic client data rates for the radio. The supported rates are those the AP will allow when setting up communications with client stations. The basic rates are the list of data rates that all stations associating with the AP must support.

Default
- 802.11a supported: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- 802.11a basic: 6, 12, 24 Mbps
- 802.11b/g supported: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
- 802.11b/g basic: 1, 2, 5.5, 11 Mbps

Format **rate** *{basic | supported} <value>*
Mode AP Profile Radio Config

Parameter	*Description*
value	A valid data rate in Mbps based on radio mode.

no rate

The **no** version of this command is used to remove a basic or supported data rate from the corresponding list.

Format **no rate** *{basic | supported} <value>*
Mode AP Profile Radio Config

Parameter	*Description*
value	A valid rate based on radio mode.

wmm

This command enables WMM mode for the radio. WMM mode is Wi-Fi Multimedia mode. When enabled QoS settings affect both downstream traffic to the station (AP EDCA parameters) and upstream traffic to the AP (station EDCA parameters). When disabled, QoS only applies to downstream traffic.

Default Enabled
Format **wmm**
Mode AP Profile Radio Config

no wmm

The **no** version of this command disables WMM mode for the radio.

Format **no wmm**
Mode AP Profile Radio Config

load-balance

This command enables load balancing. The optional utilization parameter indicates the percentage of network utilization allowed on the radio before clients are denied. *0%* indicates that no load balancing is performed.

Default
- Disabled
- utilization, 60%

Format **load-balance** *[utilization <1-100>]*
Mode AP Profile Radio Config

Parameter	*Description*
1-100	Percentage of network utilization allowed on the radio.

no load-balance

The **no** version of this command disables load balancing or resets the utilization to its default value. If no parameters are entered, load balancing is disabled.

Format **no load-balance** *[utilization]*
Mode AP Profile Radio Config

dot11n channel-bandwidth

This command selects the bandwidth used in the channel when operating in 802.11n mode.

Default 40 MHz
Format **dot11n channel-bandwidth** *{20 | 40}*
Mode AP Profile Radio Config

Parameter	*Description*
20	The Radio operates in 20 MHz bandwidth.
40	The Radio operates in 40 MHz bandwidth.

no dot11n channel-bandwidth

The **no** version of this command sets the bandwidth used to default in the channel when operating in 802.11n mode.

Format **no dot11n channel-bandwidth**
Mode AP Profile Radio Config

dot11n primary-channel

This command selects the bandwidth used in the channel when operating in 802.11n mode.

Default lower
Format **dot11n primary-channel** *{lower | upper}*
Mode AP Profile Radio Config

Parameter	*Description*
lower	The relative location of the primary channel is on the lower side in the 40 MHz channel.
upper	The relative location of the primary channel is on the upper side in the 40 MHz channel.

no dot11n primary-channel

The **no** version of this command sets the bandwidth used to the default in the channel when operating in 802.11n mode.

Format **no dot11n primary-channel**
Mode AP Profile Radio Config

protection

This command selects the protection mode to use when operating in 802.11n mode. When the protection mode is enabled, AP and stations ensure transmission is protected if there are legacy stations using the same radio frequency.

Default auto
Format **protection** *{auto | off}*
Mode AP Profile Radio Config

Parameter	*Description*
auto	The protection mechanism is set to “automatic” mode.
off	The protection mechanism is set to “off” mode.

no protection

The **no** version of this command sets the protection mechanism to the default value – automatic mode.

Format **no protection**
Mode AP Profile Radio Config

dot11n short-guard-interval

This command enables or disables the short guard interval when operating in 802.11n mode.

Default enable
Format **dot11n short-guard-interval** *{enable | disable}*
Mode AP Profile Radio Config

Parameter	*Description*
enable	The short guard interval is enabled. Guard interval is set to 400ns.
disable	The short guard interval is disabled. Guard interval is set to 800ns.

no dot11n short-guard-interval

The **no** version of this command sets the short guard interval to the default.

Format **no dot11n short-guard-interval**
Mode AP Profile Radio Config

multicast tx-rate

This command selects the rate at which the radio transmits the multicast frames.

Default auto
Format **multicast tx-rate** *<rate>*
Mode AP Profile Radio Config

Parameter	*Description*
rate	A valid rate based on the radio mode. When the radio is operating in the 5 GHz band, values are 6, 11, 12, 18, 24, 36, 48, and 54 Mbps. When the radio is operating in the 2.4 GHz band, the values are 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps. When set to 0, the multicast transmission rate selection is automatic.

no multicast tx-rate

The **no** version of this command sets the multicast transmit rate to 0.

Format `no multicast tx-rate`
Mode AP Profile Radio Config

u-apsd

This command enables the unscheduled automatic power save delivery mode for the radio.

Default Enabled
Format `u-apsd`
Mode AP Profile Radio Config

no u-apsd

The **no** version of this command disables the unscheduled automatic power save delivery mode for the radio.

Format `no u-apsd`
Mode AP Profile Radio Config

incorrect-frame-no-ack

This command configures the radio to not send any acknowledgement for incorrectly received frames.

Default Enabled
Format `incorrect-frame-no-ack`
Mode AP Profile Radio Config

no incorrect-frame-no-ack

The **no** version of this command configures the radio to send the acknowledgement for the incorrectly received frames.

Format `no incorrect-frame-no-ack`
Mode AP Profile Radio Config

show wireless ap profile radio

This command displays 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.

Format **show wireless ap profile** *<1-16>* [**radio** *<1-2> [[rates [{advertised | supported}]] | channels]]*

Mode Privileged EXEC

Parameter	*Description*
AP Profile ID	AP profile ID.
Profile Name	Descriptive name associated with the AP Profile ID.
Radio	AP profile radio interface.
Status	Indicates whether or not the radio is operational (on or off).
Mode	Indicates the physical layer technology for the radio.
RF Scan - Other Channels Mode	Indicates if the radio is configured to scan on channels other than its operating channel. A radio will always scan on its operating channel.
RF Scan - Other Channels Interval	If the radio is configured to scan other channels, indicates how often, in seconds, the radio will leave its operating channel.
RF Scan - Sentry Mode	Indicates if the radio is configured for dedicated sentry scan mode. In this mode the radio does not allow any client associations.
RF Scan – Sentry Scan Channels	Indicates which set of channels are scanned when sentry scan mode is enabled, for example, **802.11a** indicates the radio will scan all channels within the 802.11a frequency band (5 GHz).
RF Scan - Duration	Indicates how long the radio will scan on one channel. This configuration applies to both scan other channels mode and sentry scan mode.
Enable Broadcast/ Multicast Rate Limiting	Indicates if broadcast and multicast traffic rate limiting is enabled on the radio.
Broadcast/ Multicast Rate Limit	If rate limiting is enabled, broadcast/multicast traffic below this limit is transmitted normally.
Broadcast/ Multicast Rate Limit Burst	If rate limiting is enabled, broadcast/multicast traffic can occur in bursts up to this value before all traffic is considered to exceed the limit.
Beacon Interval	Interval at which the AP transmits beacon frames.
DTIM Period	Indicates the number of beacons between DTIMs (Delivery Traffic Indication Map – indicates buffered broadcast or multicast traffic on the AP).
Fragmentation Threshold	Indicates the size limit for packets transmitted over the network. Packets under configured size are not fragmented.
RTS Threshold	Indicates the number of octets in an MPDU, below which an RTS/CTS handshake shall not be performed.
Short Retry Limit	Indicates the maximum number of transmission attempts on frame sizes less than or equal to the RTS Threshold. This is a read-only value and cannot be configured.
Long Retry Limit	Indicates the maximum number of transmission attempts on frame sizes greater than the RTS Threshold. This is a read-only value and cannot be configured.
Maximum Transmit Lifetime	Indicates the elapsed time after the initial transmission of an MSDU, after which further attempts to transmit the MSDU shall be terminated. This is a read-only value and and cannot be configured.
Maximum Receive Lifetime	Indicates the elapsed time after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU shall be terminated. This is a read-only value and cannot be configured.
Maximum Clients	Maximum number of simultaneous associations allowed on the interface.

Parameter	*Description*
Automatic Channel Adjustment	Indicates if automatic channel adjustment is enabled. If enabled, the initial AP channel assignment can be automatically adjusted by the switch due to changes in the network.
Automatic Power Adjustment	Indicates if automatic power adjustment is enabled. If enabled, the switch may modify the power on the radio due to changes in performance.
Initial Power (%)	Indicates a default power setting for the radio. If automatic power adjustment is disabled, this indicates a fixed power setting, otherwise it indicates the initial power setting before any automatic adjustments.
Load Balancing	Indicates if the AP will load balance users on this radio.
Load Utilization	If load balancing is enabled, % of network utilization allowed on the radio before clients are denied.
Station Isolation	Indicates whether or not Station Isolation is enabled on the radio. When enabled the AP does not allow data traffic among wireless clients.
Channel Bandwidth	Indicates the bandwidth used in the channel when the radio is operating in 802.11n mode.
Primary Channel	Specifies the relative location of the primary channel in the 40MHz channel when the radio is operating in 802.11n mode.
Protection	Indicates if the 802.11n protection mechanism is turned on or off, or if it is in the Auto mode.
Short Guard Interval	Indicates the short guard interval configured on the radio when it is operating in 802.11n mode.
Multicast Transmit Rate	Indicates the 802.11 rate at which the radio transmits multicast frames.
Automatic Power Save Delivery Mode	Indicates if power save delivery mode is enabled or disabled on the radio.
No Ack	Indicates if acknowledgement has to be sent for incorrectly received frames.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) # show wireless ap profile 1 radio 1

AP Profile ID.................................. 1
Profile Name................................... Default
Radio.......................................... 1 - 802.11a/n
Status......................................... On
Mode........................................... 802.11a/n
RF Scan - Other Channels Mode.................. Enable
RF Scan - Other Channels Scan Interval......... 60
RF Scan - Sentry Mode.......................... Disable
RF Scan - Sentry Scan Channels................. All
RF Scan - Scan Duration........................ 10
Enable Broadcast/Multicast Rate Limiting....... Disable
Broadcast/Multicast Rate Limit................. 50
Broadcast/Multicast Rate Limit Burst........... 75
Beacon Interval................................ 100
DTIM Period.................................... 10
Fragmentation Threshold........................ 2346
RTS Threshold (bytes).......................... 2347
Short Retry Limit.............................. 7
Long Retry Limit............................... 4
Maximum Transmit Lifetime...................... 512
Maximum Receive Lifetime....................... 512
Maximum Clients................................ 200
--More-- or (q)uit
```

```
Automatic Channel Adjustment.................. Enable
Automatic Power Adjustment.................... Enable
Initial Power (%)............................. 100
Load Balancing................................ Disable
Load Utilization (%).......................... 60
Station Isolation............................. Disable
Channel Bandwidth............................. 40 MHz
Primary Channel............................... Lower
Protection.................................... Auto
Short Guard Interval.......................... Enabled
 Multicast Transmit Rate....................... Auto
Automatic Power Save Delivery Mode............. Enable
No ACK........................................ Disable

(DWS-4026) #show wireless ap profile 1 radio 2 channels

AP Profile ID................................. 1
Profile Name.................................. Default
Radio......................................... 2 - 802.11b/g
Mode.......................................... 802.11b/g

Supported Channels (* = Auto-Eligible)
-----------------------------------------------

    1*    2     3     4     5     6*    7     8

    9    10    11*
```

show wireless rates

This command displays the rates valid for a specified physical mode. This is intended to help you determine valid values for the `radio configuration` command.

Format **`show wireless rates`** *{a | bg}*

Mode Privileged EXEC

Field	*Description*
Mode	Indicates the physical layer technology to use on the radio.
Valid Rates	Indicates data rates valid for the physical mode.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless rates a

Mode.......................................... IEEE 802.11a

Valid Rates
-----------
6 Mbps
9 Mbps
12 Mbps
18 Mbps
24 Mbps
```



```
36 Mbps
48 Mbps
54 Mbps
```

show wireless multicast tx-rates

This command displays the multicast transmit rates valid for a specified physical mode. This is intended to help you determine valid values for the radio configuration command.

Format **show wireless multicast tx-rates** *{a | bg}*

Mode Privileged EXEC

Field	*Description*
Mode	Indicates the physical layer technology to use on the radio.
Valid Rates	Indicates data rates valid for the physical mode.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless rates a

Mode..................................... IEEE 802.11a

Valid Rates
-----------
6 Mbps
9 Mbps
12 Mbps
18 Mbps
24 Mbps
36 Mbps
48 Mbps
54 Mbps
```

ACCESS POINT PROFILE QOS COMMANDS

The commands in this section provide QoS configuration per radio interface and QoS queue within an access point profile.

qos ap-edca

This command configures the downstream traffic flowing from the access point to the client station EDCA queues – voice (0), video (1), best-effort (2), and background (3) queues. The command allows you to configure AIFS (Arbitration Inter-Frame Spacing), Minimum Contention Window, Maximum Contention Window, and Maximum Burst Duration for each of these queues.

Default

- ***Voice***
  AIFS, 1 msec
  Minimum Contention Window, 3 msecs
  Maximum Contention Window, 7 msecs
  Maximum Burst Duration, 1500 usec
- ***Video***
  AIFS, 1 msec
  Minimum Contention Window, 7 msecs
  Maximum Contention Window, 15 msecs
  Maximum Burst Duration, 3000 usec
- ***Best-Effort***
  AIFS, 3 msec
  Minimum Contention Window, 15 msecs
  Maximum Contention Window, 63 msecs
  Maximum Burst Duration, 0 usec
- ***Background***
  AIFS, 7 msec
  Minimum Contention Window, 15 msecs
  Maximum Contention Window, 1023 msecs
  Maximum Burst Duration, 0 usec

Format **qos ap-edca** *{background | best-effort | video | voice} {aifs <1-255> | cwmin <cwmin-time> | cwmax <cwmax-time> | max-burst <0-999900>}*

Mode AP Profile Radio Config

Parameter	*Description*
1-255	Arbitration Inter-Frame Spacing duration value in milliseconds.
cwmin-time	Minimum contention window value in milliseconds.
cwmax-time	Maximum contention window value in milliseconds.
0-999900	Maximum burst length value in microseconds.

no qos ap-edca

The **no** version of this command resets the chosen queue configuration value for AIFS, Minimum Contention Window, Maximum Contention Window, and Maximum Burst Length to its default value.

Format **no qos ap-edca** *{background | best-effort | video | voice} {aifs | cwmin | cwmax | max-burst}*

Mode AP Profile Radio Config

qos station-edca

This command configures 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 commands allow you to configure AIFS (Arbitration Inter-Frame Spacing), Minimum Contention Window, Maximum Contention Window, and Transmission Opportunity Limit for each of these queues.

Default

- ***Voice***
  AIFS, 2 msec
  Minimum Contention Window, 3 msecs
  Maximum Contention Window, 7 msecs
  Transmission Opportunity Limit, 47 msecs
- ***Video***
  AIFS, 2 msec
  Minimum Contention Window, 7 msecs
  Maximum Contention Window, 15 msecs
  Transmission Opportunity Limit, 94 msecs
- ***Best-Effort***
  AIFS, 3 msec
  Minimum Contention Window, 15 msecs
  Maximum Contention Window, 1023 msecs
  Transmission Opportunity Limit, 0 msecs
- ***Background***
  AIFS, 7 msec
  Minimum Contention Window, 15 msecs
  Maximum Contention Window, 1023 msecs
  Transmission Opportunity Limit, 0 msecs

Format **qos station-edca** *{background | best-effort | video | voice} { aifs <1-255> | cwmin <cwmin-time> | cwmax <cwmax-time> | txop-limit <0-65535> }*

Mode AP Profile Radio Config

Parameter	*Description*
1-255	Arbitration Inter-Frame Spacing duration value in milliseconds.
cwmin-time	Minimum Contention Window value in milliseconds.
cwmax-time	Maximum Contention Window value in milliseconds.
0-65535	Transmission Opportunity Limit value in milliseconds.

no qos station-edca

The **no** version of this command allows you to reset the chosen queue configuration values for AIFS, Minimum Contention Window, Maximum Contention Window, and Transmission Opportunity Limit.

Format **no qos station-edca** *{background | best-effort | video | voice} { aifs | cwmin | cwmax | txop-limit}*

Mode AP Profile Radio Config

show wireless ap profile qos

This command displays the configured values for a radio interface per QoS Queue. The various QoS queues that can be displayed are as follows:

- Background (Queue 3), lowest priority queue, high throughput.
- Best Effort (Queue 2), medium priority queue, medium throughput and delay.
- Video (Queue 1), highest priority queue, minimum delay.
- Voice (Queue 0), highest priority queue, minimum delay.

Format **show wireless ap profile** *<1-16>* radio *<1-2>* qos *[{ap-edca | station-edca}]*

Mode Privileged EXEC

Parameter	*Description*
AP Profile ID	Configured AP profile ID.
Profile Name	Name associated with the AP Profile ID.
Radio Index	AP profile radio interface.
Mode	The configured physical mode for the radio.
WMM Mode	Indicates the Wireless Multimedia mode of the radio.
Arbitration Inter-frame Spacing	AP EDCA and station EDCA wait time for data frames, ranges 1-255 milliseconds.
Minimum Contention Window	AP EDCA and station EDCA upper limit of a range from which the initial random back off wait time is determined.
Maximum Contention Window	AP EDCA and station EDCA upper limit for the doubling of the random back off value; doubling continues until either the data frame is sent or this value is reached.
Maximum Burst Length	AP EDCA maximum burst length in microseconds allowed for packet bursts on the wireless network.
Transmission Opportunity Limit	Station EDCA interval of time in milliseconds when a WME client station has the right to initiate transmissions onto the wireless medium.

Example: The following shows example CLI display output for the command.

```
Switch# show wireless ap profile 1 radio 1 qos ap-edca
AP Profile ID..................................... 1
Profile Name...................................... profile1
Radio Index....................................... 1
Mode.............................................. IEEE 802.11g
WMM Mode.......................................... Disable

QoS             AIFS   Minimum            Maximum            Maximum
Queues                 Contention Window  Contention Window  Burst
--------------  -----  -----------------  -----------------  --------
Voice (0)       1      3                  7                  1500
Video (1)       1      7                  15                 3000
Best-Effort (2) 3      15                 63                 0
Background (3)  7      15                 1023               0

Switch# show wireless ap profile 1 radio 1 qos station-edca
```



```
AP Profile ID.................................. 1
Profile Name................................... profile1
Radio Index.................................... 1
Mode........................................... IEEE 802.11g
WMM Mode....................................... Disable

QoS              AIFS   Minimum             Maximum             Tx Op
Queues                  Contention Window   Contention Window   Limit
--------------   -----  -----------------   -----------------   --------
Voice (0)        2      3                   7                   47
Video (1)        2      7                   15                  94
Best-Effort (2)  3      15                  63                  0
Background (3)   7      15                  1023                0
```

ACCESS POINT PROFILE VAP COMMANDS

The commands in this section provide Virtual Access Point (VAP) configuration per radio interface within an access point profile.

vap

This command enters the AP Profile VAP configuration mode. In this mode you can modify the VAP configuration parameters of the selected AP profile.

Format **vap** *<0-15>*
Mode AP Profile Radio Config

Parameter	*Description*
0-15	VAP ID

enable (AP Profile VAP Config Mode)

This command enables the configured VAP on the radio. VAP0 cannot be disabled; if you want to disable VAP0, you must turn off the radio.

Default VAP 0 - Enable, VAP 1-15 - Disable
Format **enable**
Mode AP Profile VAP Config

no enable

The **no** version of this command disables the configured VAP on the radio. This command is not valid for VAP 0.

Format **no enable**
Mode AP Profile VAP Config

network (AP Profile VAP Config Mode)

This command configures the network to apply to the VAP. A VAP must be configured with a network; therefore the network cannot be deleted.

Default The default networks 1-16 are applied to VAP0 – VAP15 in order.
Format **network** *<1-64>*
Mode AP Profile VAP Config

Parameter	*Description*
1-64	A configured network ID.

WS MANAGED ACCESS POINT COMMANDS

The commands in this section provide views and management of all status and statistics for an access point managed by the Unified Switch. This includes views of neighbors within the RF area for each managed AP radio interface. This section also lists commands available via Privileged EXEC mode to control the WS Managed APs.

wireless ap channel set

This command sets a new channel on the managed AP radio. The channel is not saved in the configuration, it is maintained until the next time the AP is discovered (AP or switch reset).

Format **wireless ap channel set** *<macaddr> radio <1-2> <channel>*
Mode Privileged EXEC

Parameter	*Description*
macaddr	Managed AP MAC Address.
1-2	Radio interface on the managed AP.
channel	Channel to set on the managed AP.

wireless ap debug

This command sets the admin user password and enables debug mode on the AP (this allows you telnet access to the AP, which is normally disabled in managed mode). The 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 (AP or switch reset). This command prompts for the debug password each time it is invoked.

Note: The AP admin user password will remain changed on the AP.

Default Disable
Format **wireless ap debug** *<macaddr>*
Mode Privileged EXEC

Parameter	*Description*
macaddr	Managed AP MAC Address.

no wireless ap debug

The **no** version of this command disables AP debug mode. The managed AP UI will be disabled as it normally is when the AP is in managed mode.

Format **no wireless ap debug** *<macaddr>*
Mode Privileged EXEC

wireless ap download image-type

This command sets a TFTP path and file name for the specified AP system type. The download request can be initiated for all the image types or for a specific image type. Currently the D-Link UWS supports only one image type: for DWL-8600AP.

Default None

Format **wireless ap download image-type** *img_dwl8600 <url>*

Mode Privileged EXEC

Parameter	*Description*
img_dwl8600	The image type.
url	TFTP file path for an AP system image.

Example: The following shows an example of the command.

```
(DWS-4026) #wireless ap download image-type img_dwl8600 tftp://1.1.1.1/./ap/apcode.tar ?
<cr>   Press Enter to execute the command.
```

wireless ap download group-size

This command sets the download group size. The switch requests the managed APs to download a new system image in groups. By default the switch will request the download for 10 managed APs at a time.

Default 10

Format **wireless ap download group-size** *<1-64>*

Mode Privileged EXEC

Parameter	*Description*
1-64	Enter the number of APs.

Example: The following shows an example of the command.

```
(DWS-4026) #wireless ap download group-size 3
```

wireless ap download abort

This command aborts the AP image download process. If the process is aborted, the code download still continues on the remaining APs in the current download group, but not on APs in the next download group.

Format **wireless ap download abort**

Mode Privileged EXEC

wireless ap download start

This command initiates the AP image download process to (a) all managed APs running a specific image type, or to (b) one or all managed APs irrespective of image type, to download a new system image based on the configured TFTP URL. The download is not started if the filename for the requested image type is not configured.

Format **wireless ap download start** *[image-type img_dwl8600] [<macaddr>]*
Mode Privileged EXEC

Parameter	*Description*
img_dwl8600	The image type.
macaddr	Managed AP MAC Address.

Example: The following shows an example of the command.

```
(DWS-4026) #wireless ap download start image-type img_dwl8600

(DWS-4026) #wireless ap download start

(DWS-4026) #wireless ap download start 00:00:84:00:50
```

The following text displays after you enter the command:

```
It takes about 12 minutes for the upgrade process to complete for an AP.
After this process, the AP reboots automatically and becomes managed again.
```

wireless ap power set

This command sets a new power on the managed AP radio. The power setting is not saved in the configuration, it is maintained until the next time the AP is discovered (AP or switch reset).

Format **wireless ap power set** *<macaddr>* **radio** *<1-2> <1-100>*
Mode Privileged EXEC

Parameter	*Description*
macaddr	Managed AP MAC Address.
1-2	Radio Index to be configured on the managed AP.
1-100	Power to be configured for the radio on the managed AP.

wireless ap reset

This command requests the switch to reset the managed AP indicated by the MAC address.

Format **wireless ap reset** *<macaddr>*
Mode Privileged EXEC

Parameter	*Description*
macaddr	Managed AP MAC address.

clear wireless ap failed

This command deletes one or all managed AP entries with a failed status. A failed status indicates the Unified Switch has lost contact with the managed AP.

Format **clear wireless ap failed** *[<macaddr>]*

Mode Privileged EXEC

Parameter	*Description*
macaddr	Managed AP MAC Address.

Example: The following shows an example of the command.

```
(DWS-4026) #clear wireless ap failed
Are you sure you want to clear all failed managed AP entries? (y/n) y
All managed AP failed entries cleared.
```

clear wireless ap neighbors

This command deletes entries from the managed AP client and AP neighbor lists. Note that 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 **clear wireless ap neighbors** *<macaddr>*

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(DWS-4026) #clear wireless ap neighbors
Are you sure you want to clear managed AP neighbors (associated client neighbors will not
be cleared)? (y/n) y
Managed AP neighbor entries cleared.
```

show wireless ap status

This command displays operational status for a WS managed AP. If no parameters are specified, a summary of all managed APs is displayed. If an AP MAC address is specified, the detailed status is displayed.

If the Unified Switch is a Cluster Controller, the command show all the APs managed by the peer group.

When acting as a Cluster Controller, the peer managed APs are displayed with an "*" (asterisk symbol) before the AP MAC Address in the summary command.

Format **show wireless ap** *[<macaddr>]* **status**

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
MAC Address	The Ethernet address of the WS managed AP.

Field	*Description*
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
IP Address	The network IP address of the managed AP.
IP Subnet Mask	The network mask of the managed AP.
Managing Switch	Indicates if the AP is managed by this Unified Switch or a peer Unified Switch.
Switch MAC Address	The Ethernet address of the Unified Switch managing the AP.
Switch IP Address	The network IP address of the Unified Switch managing the AP.
Status	The current managed state of the AP. The possible values are: • Discovered - The AP is discovered by the switch, but is not yet authenticated. • 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 reset.
Configuration Status	This status indicates if the AP is configured successfully with the assigned profile.
Last Failing Configuration Element	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	An ASCII string provided by the AP containing an error message for the last failing configuration element.
Debug Mode	Indicates whether or not debug mode is enabled on the AP. Debug mode allows you telnet access to the device.
Code Download Status	Iindicates the current status of a code download request for this AP.
Reset Status	Indicates the current status of an AP reset, if one has been initiated.
Profile	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 reset to configure with the new profile.
Vendor ID	Vendor of the AP software, this is learned from the AP during discovery.
Protocol Version	Indicates the protocol version supported by the software on the AP; this is learned from the AP during discovery.
Software Version	Indicates the version of software on the AP; this is learned from the AP during discovery.
Hardware Type	Hardware platform for the AP; this is learned from the AP during discovery.
Serial Number	Unique Serial number assigned to the AP; this is learned from the AP during discovery.
Part Number	Hardware part number for the AP; this is learned from the AP during discovery.

Field	*Description*
Discovery Reason	This status value indicates how the managed AP was discovered. The status is one of the following values: • IP Poll Received - The AP was discovered via an IP poll from the Unified Switch; its IP address is configured in the IP polling list. • Peer Redirect - The AP was discovered through a peer switch redirect, the AP tried to associate with another peer switch and learned the current Unified Switch IP address from the peer (peer learned Unified Switch IP address in RADIUS server response when validating the AP.) • Switch IP Configured - The managed AP is configured with the Unified Switch IP address. • Switch IP DHCP - The managed AP learned the correct Unified Switch IP address through DHCP option 43. • L2 Poll Received - The AP was discovered through the D-Link Wireless Device Discovery Protocol.
Authenticated Clients	Total number of clients currently authenticated to the AP. This is the sum of all authenticated clients for all the VAPs enabled on the AP.
System Uptime	Time in seconds since last power-on reset of the managed AP.
Age	Time since last communication between the WDS and the AP.

Example: The following shows example CLI display output for the command.

On the Cluster Controller the summary command displays entries in the following format:

```
(DWS-4026) #show wireless ap status

    MAC Address                                    Configuration
 (*) Peer Managed    IP Address    Profile Status     Status           Age
------------------ --------------- ------- ------- ------------- --------------
*00:00:85:00:50:00 192.168.37.49   1       Managed Success       0d:00:00:11

On the switch that is not acting as a Cluster Controller the summary command displays
entries in the following format:
(DWS-4026) #show wireless ap status

                                                 Configuration
   MAC Address      IP Address    Profile Status     Status           Age
----------------- --------------- ------- ------- ------------- ---------------
00:00:85:00:50:00 192.168.37.49   1       Managed Success       0d:00:00:01

(DWS-4026) #show wireless ap 00:22:B0:3A:C1:80 status

MAC address..................................... 00:22:B0:3A:C1:80
Location.........................................
IP Address...................................... 10.27.64.126
IP Subnet Mask.................................. 255.255.254.0
Managing Switch................................. Local Switch
Switch MAC Address.............................. 00:02:BC:00:00:77
Switch IP Address............................... 10.27.65.8
Status.......................................... Managed
Configuration Status............................ Success
Last Failing Configuration Element.............. None
Configuration Failure Error.....................
Debug Mode...................................... Disable
Code Download Status............................ Not Started
Reset Status.................................... Not Started
```



```
Profile..................................... 1 - Default
Vendor ID................................... D-Link
Protocol Version............................ 2
Software Version............................ D.05.22.1
Hardware Type............................... 9hw_dwl8600 - DWL-8600AP Dual Radio a/b/
g/n
Serial Number............................... H05167353
Part Number................................. dwl8600ap
Discovery Reason............................ L2 Poll Received
Authenticated Clients....................... 0
System Up Time.............................. 0d:00:02:43
Age......................................... 0d:00:00:02#
```

show wireless ap radio status

This command displays operational status for a WS managed AP radio interface. If no parameters are specified, a summary of radio status for all managed APs is displayed. If an AP MAC address and radio interface are specified, the detailed status is displayed.

Format **show wireless ap** *{<macaddr>* **radio** *[<1-2>]* **status** | **radio status***}*

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1-2	The radio interface on the AP.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates the radio interface on the AP.
Channel	If the radio is operational, the current operating channel for the radio.
Bandwidth	If the radio is operational, the current channel bandwidth in use.
Transmit Power	If the radio is operational, the current transmit power for the radio.
Associated Clients	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	Total number of neighbors (both APs and clients) that can be seen by this radio in its RF area.
Supported Channels	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	This flag indicates if 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).
Manual Channel Adjustment Status	Indicates the current state of a manual request to change the channel on this radio.
Fixed Power Indicator	This flag indicates if a fixed power setting is 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	Indicates the current state of a manual request to change the power setting on this radio.
WLAN Utilization	Indicates the total network utilization for the physical radio. This value is based on radio statistics.

Example: The following shows example CLI display output for the command.

On the Cluster Controller, the summary command will display entries in the following format:

On the switch that is not acting as a Cluster Controller the summary command displays entries in the following format:

```
(DWS-4026) #show wireless ap radio status

                                                    Transmit   Assoc.  Auth.
   MAC Address         Location        Radio Channel Power (%) Clients Clients
----------------- -------------------- ----- ------- --------- ------- -------
00:00:85:00:50:00 ap-5                 1     1       100       0       1
                                       2     153     100       0       0
(DWS-4026) show wireless ap 00:22:B0:3A:C1:80 radio 1 status

MAC address..................................... 00:22:B0:3A:C1:80
Location.........................................
Radio........................................... 1 - 802.11a/n
Supported Channels.............................. 36, 44, 52, 60, 100, 108, 116, 1
24, 132, 149, 157
Channel......................................... 149
Channel Bandwidth............................... 40 MHz
Fixed Channel Indicator......................... No
Manual Channel Adjustment Status................ Success
Transmit Power.................................. 100 %
Fixed Power Indicator........................... No
Manual Power Adjustment Status.................. Not Started
Authenticated Clients........................... 0
Total Neighbors................................. 22
WLAN Utilization................................ 4 %
```

show wireless ap radio channel status

This command displays the manual channel adjustment status for a radio on a WS managed AP. This indicates the individual AP status for a wireless channel plan apply request or a wireless AP channel set request.

Format **show wireless ap** *<macaddr>* **radio** *<1-2>* **channel status**

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1-2	Radio Interface.
Channel	If the radio is operational, the current operating channel for the radio.
Manual Channel Adjustment Status	Indicates the current state of a manual request to change the channel on this radio.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless ap 00:01:01:02:01:01 radio 2 channel status

Manual Channel Adjustment Status.............. In Progress
Channel......................................... 6

(DWS-4026) #
```


show wireless ap radio power status

This command displays the manual power adjustment status for a radio on a WS managed AP. This indicates the individual AP status for a wireless power plan apply request or a wireless AP power set request.

Format **show wireless ap** *<macaddr>* **radio** *<1-2>* **power status**

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1-2	Radio Interface.
Transmit Power	If the radio is operational, the current transmit power for the radio.
Manual Power Adjustment Status	Indicates the current state of a manual request to change the power setting on this radio.

show wireless ap radio vap status

This command displays the operational status for WS managed AP Virtual AP (VAP) interfaces. If no parameters are specified, a summary of all VAPs for a managed AP is displayed. If a VAP ID is specified, the detailed status is displayed.

Format **show wireless ap** *<macaddr>* **radio** *<1-2>* vap *[<0-15>]* **status**

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1-2	The radio interface on the AP.
0-15	VAP ID.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates a radio interface on the AP.
VAP ID	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	The Ethernet address of the VAP.
SSID	Indicates 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 Authentications	Indicates the total number of clients currently authenticated to the VAP.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless ap 00:01:01:02:01:01 radio 1 vap status

MAC address..................................... 00:01:02:03:07:10
Location.....................................
Radio........................................... 1 - 802.11a/n
```

```
                                                    Client
VAP ID   VAP MAC Address            SSID            Auth.
------ ------------------ ------------------------ ------
0      00:01:02:03:07:10   dlink1                   0
1      00:01:02:03:07:11   dlink2                   0
2      00:01:02:03:07:12   dlink3                   0
3      00:01:02:03:07:13   dlink4                   0
4      00:01:02:03:07:14   dlink5                   0
5      00:01:02:03:07:15   dlink6                   0
6      00:01:02:03:07:16   dlink7                   0
7      00:01:02:03:07:17   dlink8                   0
8      00:01:02:03:07:18   dlink9                   0
9      00:01:02:03:07:19   dlink10                  0
10     00:01:02:03:07:1A   dlink11                  0
11     00:01:02:03:07:1B   dlink12                  0
12     00:01:02:03:07:1C   dlink13                  0
13     00:01:02:03:07:1D   dlink14                  0
14     00:01:02:03:07:1E   dlink15                  0
--More-- or (q)uit
15     00:01:02:03:07:1F   dlink16                  0

(DWS-4026) #show wireless ap 00:22:B0:3A:C1:80 radio 1 vap 2 status

MAC address..................................... 00:22:B0:3A:C1:80
Location.....................................
Radio........................................... 1
VAP ID.......................................... 2
VAP MAC Address................................. 00:22:B0:3A:C1:80
SSID............................................ dlink1
Client Authentications.......................... 0
```

show wireless ap radio neighbor ap status

This command displays the status parameters for each neighbor AP detected through an RF scan on the specified managed AP radio.

Format **show wireless ap** *<macaddr>* **radio** *<1-2>* **neighbor ap status**

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1-2	The radio interface on the AP.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates a radio interface on the AP.
Neighbor AP MAC	The Ethernet MAC address of the neighbor AP network, this could be a physical radio interface or VAP MAC address. For D-Link APs, this is always a VAP MAC address. The neighbor AP MAC address may be cross-referenced in the RF Scan status.
SSID	Service Set ID of the neighbor AP network.

Field	*Description*
RSSI	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	Indicates 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	Indicates the time since this AP was last reported from an RF scan on the radio.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless ap 00:01:01:02:01:01 radio 1 neighbor ap status

MAC Address..................................... 00:01:01:02:01:01
Location........................................ FirstFloor
Radio........................................... 1

 Neighbor AP MAC              SSID              RSSI     Status          Age
----------------- --------------------------- ---- --------------- -----------
00:01:01:02:01:03 Network3                    10   Managed         0h:2m:52s
00:01:01:02:03:02 Network2                    10   Managed         0h:2m:55s
00:33:01:02:01:83 Lobby                       10   Unknown         0h:2m:49s
```

show wireless ap radio neighbor client status

This command displays the status parameters for each client detected as a neighbor to the specified managed AP radio. A client neighbor may be detected through one or more methods: RF scan on the radio, client association to a VAP on the radio, or receiving a probe request from the client.

Format **show wireless ap** *<macaddr>* **radio** *<1-2>* **neighbor client status**

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1-2	The radio interface on the AP.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates a radio interface on the AP.
Neighbor Client MAC	The Ethernet address of the client station.
RSSI	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.

Field	*Description*
Channel	The managed AP channel the client frame was received on, which may be different than the operating channel for this radio.
Discovery Reason	Indicates 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.
Age	Indicates the time since this client was last reported from an RF scan on the radio.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless ap 00:01:01:02:01:01 radio 1 neighbor client status

MAC Address..................................... 00:01:01:02:01:01
Location........................................ FirstFloor
Radio........................................... 1

Neighbor MAC      RSSI Channel Discovery Reason           Age
----------------- ---- ------- -------------------------- ----------------
00:01:01:10:01:01 20   6       Assoc this AP,Probe        00d:00h:05m:21s
00:01:01:14:01:01 20   6       Assoc this AP,Probe        00d:00h:05m:20s
00:01:31:16:01:01 20   11      Probe,RF                   00d:00h:05m:19s
```

show wireless ap statistics

This command displays global statistics for a managed AP, the managed AP MAC address parameter is required, and the command displays a detailed view of the current statistics. You can clear all wireless statistics through the `clear wireless statistics` command.

Format **`show wireless ap`** *<macaddr>* **`statistics`**

Mode Privileged EXEC

Field	*Description*
macaddr	Managed AP MAC address.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server.)
WLAN Packets Received	The total packets received by the AP on the wireless network.
WLAN Bytes Received	Total bytes received by the AP on the wireless network.

Field	*Description*
WLAN Packets Transmitted	Total packets transmitted by the AP on the wireless network.
WLAN Bytes Transmitted	Total bytes transmitted by the AP on the wireless network.
WLAN Packets Receive Dropped	Total receive packets discarded by the AP on the wireless network.
WLAN Bytes Received	Total receive bytes discarded by the AP on the wireless network.
WLAN Packets Transmitted	Total packets discarded by the AP prior to transmission on the wireless network.
WLAN Bytes Transmitted	Total bytes discarded by the AP prior to transmission on the wireless network.
Ethernet Packets Received	Total packets received by the AP on the wired network.
Ethernet Bytes Received	Total bytes received by the AP on the wired network.
Ethernet Multicast Packets Received	Total multicast packets received by the AP on the wired network.
Ethernet Packets Transmitted	Total packets transmitted by the AP on the wired network.
Ethernet Bytes Transmitted	Total bytes transmitted by the AP on the wired network.
Total Transmit Errors	Total transmit errors detected by the AP on the wired network.
Total Receive Errors	Total receive errors detected by the AP on the wired network.
ARP Reqs Converted from Bcast to Ucast	Total number of ARP request converted from broadcast to unicast on the wireless netework.
Filtered ARP Requests	Total number of ARP requests filtered by the AP instead of sending on the wireless network.
Broadcasted ARP Requests	Total number of ARP requests broadcasted on the wireless network after performing wireless ARP suppression.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless ap 00:01:01:02:01:01 statistics

MAC Address..................................... 00:01:01:02:01:01
Location........................................ FirstFloor
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
Ethernet Packets Received....................... 0
Ethernet Packets Transmitted.................... 0
```

```
Ethernet Bytes Received..................... 0
Ethernet Bytes Transmitted.................. 0
Ethernet Multicast Packets Received......... 0
Total Transmit Errors....................... 0
Total Receive Errors........................ 0
ARP Reqs Converted from Bcast to Ucast..... 50
Filtered ARP Requests....................... 8
Broadcasted ARP Requests.................... 5

(DWS-4026) #
```

show wireless ap radio statistics

This command displays statistics for each physical radio on a WS managed AP, the managed AP MAC address and radio parameters are required, the command displays a detailed view of the current statistics.

Format **show wireless ap** *<macaddr>* **radio** *<1-2>* **statistics**

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1-2	The radio interface on the AP.
MAC Address	The Ethernet address of the WS managed AP.
Location	A description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates a radio interface on the AP.
WLAN Packets Received	Total packets received by the AP on this radio interface.
WLAN Bytes Received	Total bytes received by the AP on this radio interface.
WLAN Packets Transmitted	Total packets transmitted by the AP on this radio interface.
WLAN Bytes Transmitted	Total bytes transmitted by the AP on this radio interface.
WLAN Packets Receive Dropped	Total receive packets discarded by the AP on this radio interface.
WLAN Bytes Received	Total receive bytes discarded by the AP on this radio interface.
WLAN Packets Transmitted	Total packets discarded by the AP prior to transmission on this radio interface.
WLAN Bytes Transmitted	Total bytes discarded by the AP prior to transmission on this radio interface.
Transmitted Fragment Count	Count of acknowledged MPDU with an individual address or an MPDU with a multicast address of type Data or Management.
Multicast Transmitted Frame Count	Count of successfully transmitted MSDU frames where the multicast bit is set in the destination MAC address.

Field	*Description*
Failed Count	Number of times an MSDU is not transmitted successfully due to transmit attempts exceeding either the short retry limit or the long retry limit.
Retry Count	Number of time an MSDU is successfully transmitted after one or more retries.
Multiple Retry Count	Number of times an MSDU is successfully transmitted after more than one retry.
Frame Duplicate Count	Number of times a frame is received and the Sequence Control field indicates it is a duplicate.
RTS Success Count	Count of CTS frames received in response to an RTS frame.
RTS Failure Count	Count of CTS frames not received in response to an RTS frame.
ACK Failure Count	Count of ACK frames not received when expected.
Received Fragment Count	Count of successfully received MPDU frames of type data or management.
Multicast Received Frame Count	Count of MSDU frames received with the multicast bit set in the destination MAC address.
FCS Error Count	Count of FCS errors detected in a received MPDU frame.
Transmitted Frame Count	Count of each successfully transmitted MSDU.
WEP Undecryptable Count	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.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless ap 00:01:01:02:01:01 radio 1 statistics

MAC Address..................................... 00:01:01:02:01:01
Location........................................ FirstFloor
Radio........................................... 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
Fragments Received.............................. 0
Fragments Transmitted........................... 0
Multicast Frames Received....................... 0
Multicast Frames Transmitted.................... 0
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................................. 0
Frames Transmitted.............................. 0
WEP Undecryptable Count......................... 0
```

show wireless ap radio vap statistics

This command displays statistics for each VAP on a WS managed AP radio. All parameters are required, and the command displays a detailed view of the current statistics.

Format	**show wireless ap** *<macaddr>* **radio** *<1-2>* **vap** *<0-7>* **statistics**
Mode	Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1-2	The radio interface on the AP.
0-7	VAP ID.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates a radio interface on the AP.
VAP	Indicates the VAP ID on the radio.
WLAN Packets Received	Total packets received by the AP on this VAP.
WLAN Bytes Received	Total bytes received by the AP on this VAP.
WLAN Packets Transmitted	Total packets transmitted by the AP on this VAP.
WLAN Bytes Transmitted	Total bytes transmitted by the AP on this VAP.
WLAN Packets Receive Dropped	Total receive packets discarded by the AP on this VAP.
WLAN Bytes Received	Total receive bytes discarded by the AP on this VAP.
WLAN Packets Transmitted	Total packets discarded by the AP prior to transmission on this VAP.
WLAN Bytes Transmitted	Total bytes discarded by the AP prior to transmission on this VAP.
Client Association Failures	Number of clients that have been denied association to the VAP.
Client Authentication Failures	Number of clients that have failed authentication to the VAP.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless ap 00:01:01:02:01:01 radio 1 vap 1 statistics

AP MAC Address.................................. 00:01:01:02:01:01
Location........................................ FirstFloor
Radio........................................... 1
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
```

show wireless ap download

This command displays global configuration and status for an AP code download request. It does not accept any parameters.

Format `show wireless ap download`

Mode Privileged EXEC

Field	*Description*
Image File Name	The AP image filename on the TFTP server.
Image File Path	The AP image file path on the TFTP server.
Server Address	The TFTP server IP address.
Group Size	If a code download request is for all managed APs, the switch processes the request for one group of APs at a time before starting the next group. The group size indicates the maximum number of APs the switch will send the code download request to at one time.
Download Type	The last download type requested.
Download Status	The global status for the code download request.
Total Count	The total number of managed APs being updated in the current code download request. This may be one AP or the total number of managed APs at the time a code download request is started.
Success Count	Indicates the total number of managed APs that have successfully downloaded their code for the current code download request.
Failure Count	Indicates the total number of managed APs that have failed to download their code for the current code download request.
Abort Count	Indicates the number of APs for which the download was aborted, starting at 0 and incrementing with each aborted download.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless ap download

Image File Name.............................
Image File Path.............................
Server Address..............................
Group Size..................................... 10
Download Type.................................. All images
Download Status................................ Not Started
Total Count.................................... 0
Success Count.................................. 0
Failure Count.................................. 0
Abort Count.................................... 0
```

show wireless ap radio radar status

This command displays radar status for each radio on a WS managed AP. All parameters are required. The radar status is displayed for mode **a** radios only. For **b/g** mode radios, an error is displayed.

Format **show wireless ap** *<mac-addr>* **radio** *<1-2>* **radar status**

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address
1-2	The radio interface on the AP.
Channel	The list of channels available on the specified radio.
Radar Detection Required	In some regulatory domains, 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	Indicates whether another 802.11 device was detected on the channel.
Last Radar Detected Time	Shows the amount of time that has passed since the device was last detected on the channel.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless ap 00:22:B0:3A:C1:80 radio 1 radar status

          Radar Detection    Radar Detected     Last Radar
Channel      Required            Status        Detected Time
------- ------------------- ---------------- ----------------
36      No                  No               0d:00:00:00
44      No                  No               0d:00:00:00
52      Yes                 No               0d:00:00:00
60      Yes                 No               0d:00:00:00
100     Yes                 No               0d:00:00:00
108     Yes                 No               0d:00:00:00
116     Yes                 No               0d:00:00:00
124     Yes                 No               0d:00:00:00
132     Yes                 No               0d:00:00:00
149     No                  No               0d:00:00:00
157     No                  No               0d:00:00:00
```


ACCESS POINT FAILURE STATUS COMMANDS

The commands in this section provide views and management of data maintained for access point association and authentication failures.

clear wireless ap failure list

This command deletes all entries from the AP failure list, entries 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 Unified Switch.

Format	**`clear wireless ap failure list`**
Mode	Privileged EXEC

Example: The following shows an example of the command.

```
(DWS-4026) #clear wireless ap failure list
Are you sure you want to clear the entire AP failure list? (y/n) y
All AP failure entries cleared.

(DWS-4026) #clear wireless ap failure list
Are you sure you want to clear the entire AP failure list? (y/n) n
AP failure entries not cleared.
```

show wireless ap failure status

This command displays summary or detailed data for entries in the AP failure list. Entries are added to the list when the Unified Switch fails to validate or authenticate an AP.

When acting as a Cluster Controller, the peer Unified Switch reported AP failures are also displayed. To identify such entries in the summary command display, a "*" (asterisk) is used alongside the peer Unified Switch reported AP MAC Address.

Format	**`show wireless ap`** *`[<macaddr>]`* **`failure status`**
Mode	Privileged EXEC

Field	*Description*
macaddr	The failure AP MAC address.
MAC Address	The Ethernet address of the AP.
IP Address	The network IP address of the AP.
Reporting Switch	Indicates if AP Failure happened with this Unified Switch or peer Unified Switch.
Switch MAC Address	The Ethernet address of the Unified Switch managing the AP.
Switch IP Address	The network IP address of the Unified Switch managing the AP.
Last Failure Type	Indicates the last type of failure that occurred. If the WS supports the Integrated AP image download mode and the AP auto upgrade is enabled, the AP is automatically upgraded upon discovery. However, if no AP image is found on the WS to upgrade the AP, this failure type is reported as 'AP Code Image Not Available'.
Validation Failure Count	The count of association failures for this AP.

Field	*Description*
Authentication Failure Count	The count of authentication failures for this AP.
Vendor ID	Vendor of the AP software.
Protocol Version	Indicates the protocol version supported by the software on the AP.
Software Version	Indicates the version of software on the AP.
Hardware Type	Hardware platform for the AP.
Age	Time in seconds since failure occurred.

Example: The following shows example CLI display output for the command.

On the Cluster Controller, the summary command will display entries in the following format:

```
(DWS-4026) #show wireless ap failure status

    MAC Address
 (*) Peer Managed   IP Address       Last Failure Type           Age
------------------ --------------- ----------------------- ----------------
*00:00:86:00:50:00 192.168.37.74   No Database Entry        0d:00:00:06

On the switch that is not acting as a Cluster Controller the summary command displays
entries in the following format:

(DWS-4026) #show wireless ap failure status

   MAC Address      IP Address       Last Failure Type           Age
----------------- --------------- ----------------------- ----------------
00:00:85:00:50:00 192.168.37.49   No Database Entry        0d:00:02:02
00:00:86:00:50:00 192.168.37.74   No Database Entry        0d:00:00:03


(DWS-4026) #show wireless ap 00:22:B0:3A:C8:40 failure status

MAC address.............................. 00:22:B0:3A:C8:40
IP Address............................... 10.27.64.163
Reporting Switch......................... Local Switch
Switch MAC Address....................... 00:02:BC:00:00:77
Switch IP Address........................ 10.27.65.8
Last Failure Type........................ No Database Entry
Validation Failure Count................. 6
Authentication Failure Count............. 0
Vendor ID................................ D-Link
Protocol Version......................... 2
Software Version......................... D.06.04.1
Hardware Type............................ hw_dwl8600 - DWL-8600AP Dual Radio a/b/g/n
Age...................................... 0d:00:00:29
```


RF SCAN ACCESS POINT STATUS COMMANDS

The commands in this section provide views and management of data maintained for all access points known by the Unified Switch via RF scan data obtained from the managed access points.

clear wireless ap rf-scan list

This command deletes all entries from the RF scan list; entries normally age out according to the configured age time.

Format	**`clear wireless ap rf-scan list`**
Mode	Privileged EXEC

Example: The following shows an example of the command.

```
(DWS-4026) #clear wireless ap rf-scan list
Are you sure you want to clear all RF scan entries? (y/n) y
All RF scan entries cleared.
```

show wireless ap rf-scan status

This command displays summary or detailed data for APs detected via RF scan on the managed APs. If the optional MAC address parameter is specified, detailed data is displayed.

Format	**`show wireless ap`** *`[<macaddr>]`* **`rf-scan status`**
Mode	Privileged EXEC

Field	*Description*
macaddr	AP MAC address detected in RF scan.
MAC Address	The Ethernet MAC address of the detected AP, this could be a physical radio interface or VAP MAC. For D-Link APs, this is always a VAP MAC address.
BSSID	Basic Service Set Identifier advertised by the AP in the beacon frames.
SSID	Service Set ID of the network, this is broadcast in the detected beacon frame.
OUI	Vendor name for the MAC address.
Physical Mode	Indicates the 802.11 mode being used on the AP.
Channel	Transmit channel of the AP.
Status	Indicates 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	Time in seconds since this AP was last detected in an RF scan.
The following parameters are displayed only in the detailed status:	
Transmit Rate	Indicates the rate at which the AP is currently transmitting data.

Field	*Description*
Beacon Period	Beacon interval for the neighbor AP network.
Initial Status	If the AP is not rogue, then initial status is equal to “Status”. For rogue APs, the initial status is the classification prior to this AP becoming rogue. 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).
AP MAC Address	If status indicates a managed AP, this indicates the base MAC address of the AP.
Radio Interface	If status indicates a managed AP, this indicates the radio interface on the AP.
Discovered Age	Time in seconds since this AP was first detected in an RF scan.
Security Mode	Security used by this AP: Open, WEP, or WPA.
Highest Supported Rate	The highest supported rate advertised by this AP in the beacon frames. An integer value representing the number per 100Kbps.
802.11n Mode	Flag indicating whether this AP supports 802.11n.
Ad Hoc Network	Flag indicating that the beacon frame is received from an Ad hoc network. Possible values are: **false**-Not Ad hoc, **true**-Ad hoc.
Peer Managed AP	Flag indicating this AP is managed by a peer switch. Valid values are: • Locally managed - AP is managed by the local switch. • Peer managed - AP is managed by a peer switch.
Rogue Mitigation	Status indicating whether rogue AP mitigation is in progress for this AP. If mitigation is not in progress then this field displays the reason, which can be one of the following: • Not Required (AP s not rogue) • Already mitigating too many APs. • AP Is operating on an illegal channel. • AP is spoofing valid managed AP MAC address. • AP is Ad hoc.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless ap rf-scan status

                                  Physical                          Discovered
   MAC Address          SSID        Mode   Channel     Status          Age
----------------- ---------------- -------- ------- --------------- -----------
00:01:01:02:01:03 Network3         802.11g  6       Managed         3h:28m:11s
00:01:01:02:03:02 Network2         802.11g  6       Managed         3h:28m:14s
00:33:01:02:01:83 Lobby            802.11g  6       Unknown         3h:28m:8s

(DWS-4026) #show wireless ap 00:11:95:A3:7A:C8 rf-scan status

MAC Address..................................... 00:11:95:A3:7A:C8
SSID............................................ Guest Network
OUI............................................. Unknown
Physical Mode................................... 802.11g
Channel......................................... 1
Status.......................................... Rogue
Initial Status.................................. Rogue
```



```
Transmit Rate (Mpbs)..... 1 Mbps
Beacon Period (msecs)..... 100
Discovered Age..... 0d:00:03:01
Age..... 0d:00:02:57
Security Mode..... Open
Highest Supported Rate (per 100Kbps)..... 10
802.11n Mode..... Supported
Ad hoc Network..... Not Ad hoc
Rogue Mitigation..... Not Required

(DWS-4026) #
```

show wireless ap rf-scan triangulation

This command displays the signal triangulation status for the specified RF scan entry. Triangulation information is provided to help locate the rogue AP by showing which managed APs detect each device discovered through the RF Scan. Up to six triangulation entries are reported for each AP detected through the RF Scan: three entries by non-sentry APs and three entries by sentry APs. Since an AP may have one radio configured in sentry mode and another radio configured in non-sentry mode, the same AP can appear in both lists. If the AP has not been detected by three APs, then the list may contain zero, one, or two entries.

Format **show wireless ap** <*macaddr*> **rf-scan triangulation**

Mode Privileged EXEC

Field	*Description*
macaddr	AP MAC address detected in RF scan.
Sentry	Identifies whether the AP that detected the entry is in sentry or non-sentry mode.
MAC Address	Shows the MAC address of the AP that detected the RF Scan entry. The address links to the valid AP database.
Radio	Identifies the radio on the AP that deleted the RF Scan entry.
RSSI	Shows the received signal strength indicator (RSSI) in terms of percentage for the non-sentry AP. The range is 0, which means the AP is not detected, to 100%.
Signal (dBm)	Received signal strength for the non-sentry AP. The range is -127 dBm to 127 dBm, but most values are expected to be range from -95 dBm to -10 dBm.
Noise (dBm)	Noise reported on the channel by the non-sentry AP.
Age	Time since this AP was last detected in an RF scan.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless ap 00:02:BC:00:17:D0 rf-scan triangulation

                                  RSSI Signal Noise
  Sentry      MAC Address    Radio (%)  (dBm)  (dBm) Age
---------- ----------------- ----- ---- ------ ----- -----------
Non-Sentry 00:22:B0:3A:C1:80   2     15    -80   -92 0d:15:48:19
```

show wireless ap rf-scan rogue-classification

This command displays the WIDS AP rogue classification test results.

Format **show wireless ap** <*macaddr*> **rf-scan rogue-classification**

Mode Privileged EXEC

Field	*Description*
macaddr	AP MAC address detected in RF scan.
Test ID	Test identifier (WIDSAPROGUEnn).
Cond Detect	Indicates whether this test detected the condition that it is designed to detect. Valid values are **True** or **False**.
MAC Addr (radio)	The Managed AP MAC address and (radio number) that last reported detecting this condition.
Test Config	Indicates whether this test is configured to report rogues. Valid values are **Enable** or **Disable**.
Test Result	Indicates whether this test reported the device as rogue. Valid values are **Rogue** or empty string.
Time Since 1st Report	Time stamp indicating how long ago this test first detected the condition.
Time Since Last Report	Time stamp indicating how long ago this test last detected the condition.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) # show wireless ap 00:11:95:A3:7A:C8 rogue-classification

              Cond                          Test    Test   Time Since  Time Since
Test ID       Detect MAC Addr (radio)       Config  Result 1st Report  Last Report
------------- ------ ---------------------- ------- ------ ----------- -----------
WIDSAPROGUE01 True   00:00:00:00:00:11(1) Enable  Rogue  0d:00:00:00 0d:00:00:01
WIDSAPROGUE02 False  00:00:00:00:00:12(2) Disable        0d:00:00:00 0d:00:00:00
WIDSAPROGUE03 True   00:00:00:00:00:13(0) Enable  Rogue  0d:00:00:02 0d:00:00:03
WIDSAPROGUE04 True   00:00:00:00:00:14(1) Enable  Rogue  0d:00:00:04 0d:00:00:05
WIDSAPROGUE05 True   00:00:00:00:00:15(2) Enable  Rogue  0d:00:00:06 0d:00:00:07
WIDSAPROGUE06 True   00:00:00:00:00:16(0) Enable  Rogue  0d:00:01:28 0d:00:01:39
WIDSAPROGUE07 False  00:00:00:00:00:17(1) Enable         0d:00:01:51 0d:00:03:42
WIDSAPROGUE08 False  00:00:00:00:00:18(2) Enable         0d:00:05:33 0d:00:07:24
WIDSAPROGUE09 False  00:00:00:00:00:19(2) Enable         0d:00:09:15 0d:00:11:06
WIDSAPROGUE10 False  00:00:00:00:00:1A(0) Enable         0d:00:12:57 0d:00:14:48
WIDSAPROGUE11 False  00:00:00:00:00:1B(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
WIDSAPROGUE10..... Unexpected WDS device detected on network
WIDSAPROGUE11..... Unmanaged AP detected on wired network
```


CLIENT ASSOCIATION STATUS AND STATISTICS COMMANDS

The commands in this section provide views and management of all status and statistics for wireless clients. In addition to commands to display data from the associated client perspective, this section includes commands to display a view of all clients associated to a specific VAP, and to display a view of all clients associated to a specific SSID.

wireless client disassociate

This command initiates a request to disassociate a client associated to a managed AP specified by the client MAC address. The Unified Switch will send a message to the appropriate managed AP to force the disassociation.

Format `wireless client disassociate <macaddr>`

Mode Privileged EXEC

Parameter	*Description*
macaddr	Client MAC address.

show wireless client status

This commands displays summary or detailed data for clients associated to a managed AP. If the Unified Switch is a Cluster Controller, the command shows 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 [<macaddr>] status`

Mode Privileged EXEC

Parameter	*Description*
macaddr	Client MAC address.

The command output displays the following information.

Field	*Description*
MAC Address	The Ethernet address of the client station.
Detected IP Address	This is the IPv4 address detected for the clents using ARP snooping.
Tunnel IP Address	This field is blank for all non-tunneled clients. For a tunneled client, this is the assigned tunnel IP address.
Associating Switch	Indicates if the client is associated to an AP managed by this Unified Switch or a peer Unified Switch.
Switch MAC Address	The Ethernet address of the Unified Switch associating this client.
Switch IP Address	The network IP address of the Unified Switch associating this client.
SSID	Indicates the network on which the client is connected.
NetBIOS Name	NetBIOS name of the client.
VAP MAC Address	Indicates the Ethernet MAC address for the managed AP VAP where this client is associated.

Field	*Description*
Channel	Indicates the operating channel for the client association.
Status	Indicates 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.
AP MAC Address	This field indicates the base AP Ethernet MAC address for the managed AP.
Location	The descriptive location configured for the managed AP.
Radio	Displays the managed AP radio interface on which the client is associated.
VLAN	If the client is on a VAP using VLAN data forwarding mode, indicates the current assigned VLAN.
User Name	Indicates the user name of clients that have authenticated via 802.1x. Clients on networks with other security modes will not have a user name.
Transmit Data Rate	Indicates the rate at which the client station is currently transmitting data.
802.11n-Capable	For current association, this flag indicates whether the client is capable of 802.11n operation.
Inactive Period	For current association, the period of time that the AP has not seen any traffic for the client.
Age	Indicates the time in seconds since the switch received new status or statistics update for this client.
Network Time	Indicates the time since the client first authenticated with the network.

Example: The following shows example CLI display output for the command.

On the Cluster Controller the summary command displays entries in the following format:

```
(DWS-4026) #show wireless client status

    MAC Address
 (*) Peer Managed   VAP MAC Address        SSID        Status    Network Time
------------------ ----------------- ----------------- --------- --------------
*00:0F:B5:86:93:95 00:00:86:00:50:00 l7network         Auth      0d:01:09:52
 00:0F:B5:88:93:95 00:00:88:00:50:00 l7network         Auth      0d:01:09:52

(DWS-4026) #

On the switch that is not acting as a Cluster controller the summary command displays
entries in the following format:
(DWS-4026) #show wireless client status

    MAC Address     VAP MAC Address        SSID        Status    Network Time
------------------ ----------------- ----------------- --------- --------------
 00:0F:B5:86:93:95 00:00:86:00:50:00 l7network         Auth      0d:01:09:52

(DWS-4026) #
```

Example: The following shows CLI display output for a particular MAC address:

```
(DWS-4026) #show wireless client 00:14:6c:59:d1:99 status

MAC address..................................... 00:14:6C:59:D1:99
Detected IP Address............................. -----
Detected IP Address............................. -----
VAP MAC Address................................. 00:02:BC:00:17:D0
AP MAC Address.................................. 00:02:BC:00:17:D0
```



```
Location.....................................
Radio.......................................... 2 - 802.11b/g/n
Associating Switch............................. Local Switch
Switch MAC Address............................. 00:FC:E3:90:01:07
Switch IP Address.............................. 10.27.64.121
Tunnel IP Address.............................. -----
SSID........................................... ALT-VLAN-8
NetBIOS Name................................... PCRDU-ATSIGLER
Status......................................... Authenticated
Channel........................................ 1
User Name.....................................
VLAN........................................... 8
Transmit Data Rate............................. 1 Mbps
802.11n Capable................................ No
STBC Capable................................... No
Inactive Period................................ 0d:00:00:55
Age............................................ 0d:00:00:04
Network Time................................... 0d:23:32:51

(DWS-4026) #
```

show wireless client summary

This commands displays brief summary of clients associated to a managed AP.

If the WS is a WIDS Controller, the command shows all the associated clients in the peer-group.

When acting as WIDS Controller, the peer switch associated clients are displayed with a "*" before the Client MAC Adress in the summary command.

Format	**`show wireless client summary`**
Mode	Privileged EXEC

The command output displays the following information:

Field	*Description*
MAC Address	The Ethernet address of client station.
IP Address	This is the IPv4 address detected for the cilents using ARP snooping.
NetBIOS Name	NetBIOS Name of the client.

Example: On the WIDS Controller the summary command displays entries in the following format:

```
(DWS-4026) #show wireless client summary

    MAC Address
(*) Peer Managed   IP Address        NetBIOS Name
------------------ ----------------- -----------------
*00:0F:B5:86:93:95 8.0.1.29          l7client-01
 00:0F:B5:86:93:96 8.0.1.29          l7client-02

(DWS-4026) #
```

On the switch that is not acting as a WIDS Controller the summary command displays entries

```
in the following format:
(DWS-4026) #show wireless client summary

    MAC Address    IP Address        NetBIOS Name
------------------ ----------------- -----------------
 00:0F:B5:86:93:95 8.0.1.29          l7client-01
 00:0F:B5:86:93:96 8.0.1.29          l7client-02
```

show wireless client client-qos status

This command displays detailed client QoS data for clients associated to a managed AP. These are the current operational values in effect for the specified client.

Format **show wireless client** *<macaddr>* **client-qos status**

Mode Privileged EXEC

Field	*Description*
macaddr	Client MAC address.
MAC Address	The Ethernet address of the client station.
SSID	The network on which the client is connected.
Client QoS Operational Status	Indicates whether or not the client is performing client QoS operations. Possible values are **Enabled** or **Disabled**.
Bandwidth Limit Down	The maximum transmission rate limit in bits per second in effect for traffic flowing from the AP to the client. This may differ from the configured value due to rounding. A value of 0 indicates no rate limiting is in effect in this direction.
Bandwidth Limit Up	The maximum transmission rate limit in bits per second in effect for traffic flowing from the client to the AP. This may differ from the configured value due to rounding. A value of 0 indicates no rate limiting is in effect in this direction.
Access Control Down	Identifies the access control list in effect for traffic flowing from the AP to the client. Both the ACL type and its name (or number) is displayed. A value of *<none>* indicates no access control is in effect in this direction.
Access Control Up	Identifies the access control list in effect for traffic flowing from the client to the AP. Both the ACL type and its name (or number) is displayed. A value of *<none>* indicates no access control is in effect in this direction.
Diffserv Policy Down	Identifies the Diffserv policy in effect for traffic flowing from the AP to the client. A value of *<none>* indicates no policy is in effect in this direction.
Diffserv Policy Up	Identifies the Diffserv policy in effect for traffic flowing from the client to the AP. A value of *<none>* indicates no policy is in effect in this direction.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless client 00:0F:B5:86:93:95 client-qos status

MAC Address..................................... 00:0F:B5:86:93:95
SSID............................................ l7network
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>
```

show wireless client client-qos radius status

This command displays detailed client QoS data for clients associated to a managed AP. These are the configured values successfully obtained from a RADIUS server for the specified client.

Format **show wireless client** *<macaddr>* **client-qos radius status**

Mode Privileged EXEC

Field	*Description*
macaddr	Client MAC address.
MAC Address	The Ethernet address of the client station.
SSID	The network on which the client is connected.
Bandwidth Limit Down	Defines the maximum transmission 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. A value of *<none>* indicates that this parameter was not obtained from RADIUS for the client.
Bandwidth Limit Up	Defines the maximum transmission 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. A value of *<none>* indicates that this parameter was not obtained from RADIUS for the client.
Access Control Down	Defines the configured 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. A value of *<none>* indicates that this parameter was not obtained from RADIUS for the client.
Access Control Up	Defines the 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. A value of *<none>* indicates that this parameter was not obtained from RADIUS for the client.
Diffserv Policy Down	Defines the Diffserv policy to use for traffic flowing from the AP to the client. A value of *<none>* indicates that this parameter was not obtained from RADIUS for the client.
Diffserv Policy Up	Defines the Diffserv policy to use for traffic flowing from the client to the AP. A value of *<none>* indicates that this parameter was not obtained from RADIUS for the client..

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless client 00:0F:B5:86:93:95 client-qos radius status

MAC Address................................. 00:0F:B5:86:93:95
SSID........................................ l7network
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-4026) #
```

show wireless client statistics

This command displays association or session statistics for clients currently associated with a WS managed AP. The session statistics show the cumulative association values if a client roams across managed APs. If no optional parameters are specified, the session statistics are displayed.

Format **show wireless client** <*macaddr*> **statistics** [{association | session}]

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP's client MAC address.
MAC Address	The Ethernet address of the client station.
Packets Received	Total packets received from the client station.
Bytes Received	Total bytes received from the client station.
Packets Transmitted	Total packets transmitted to the client station.
Bytes Transmitted	Total bytes transmitted to the client station.
Packets Receive Dropped	Total receive packets from the client station that were discarded by the AP.
Bytes Receive Dropped	Total receive bytes from the client station that were discarded by the AP.
Packets Transmit Dropped	Totals packets discarded by the AP prior to transmission to the client station.
Bytes Transmit Dropped	Total bytes discarded by the AP prior to transmission to the client station.
Duplicate Packets Received	Total duplicate packets received from the client station.
Packet Fragments Received	Total fragmented packets received from the client station.
Packet Fragments Transmitted	Total fragmented packets transmitted to the client station.
Transmit Retry Count	Number of times transmits to the client station succeeded after one or more retries.
Transmit Retry Failed Count	Number of times transmits to the client station failed after one or more retries.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless client 00:01:01:10:01:01 statistics

MAC Address..................................... 00:01:01:10:01:01
Packets Received................................ 0
Packets Transmitted............................. 0
Bytes Received.................................. 0
Bytes Transmitted............................... 0
Packets Receive Dropped......................... 0
Packets Transmit Dropped........................ 0
Bytes Receive Dropped........................... 0
Bytes Transmit Dropped.......................... 0
Duplicate Packets Received...................... 0
Packet Fragments Received....................... 0
Packet Fragments Transmitted.................... 0
Transmit Retry Count............................ 0
Failed Retry Count.............................. 0
```



```
(DWS-4026) #
```

show wireless client neighbor ap status

This command displays all the APs an associated client can see in its RF area; for associated clients this provides a reverse view of the managed AP client neighbor list. It allows you to view where a client may roam based on its neighbor APs.

Format **show wireless client** *<macaddr>* **neighbor ap status**

Mode Privileged EXEC

Field	*Description*
macaddr	Client MAC address.
MAC Address	The Ethernet address of the client station.
AP MAC Address	The base Ethernet address of the WS managed AP.
Location	The configured descriptive location for the managed AP.
Radio	The radio on the managed AP that detected this client as a neighbor.
Discovery Reason	Indicates 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.

show wireless vap client status

This command displays 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 status**

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP VAP MAC address.
VAP MAC Address	Indicates the Ethernet MAC address for the managed AP VAP where this client is associated.
MAC Address	The Ethernet address of client station.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless vap 00:02:03:04:05:08 client status
VAP MAC Address    Client MAC Address
-----------------  ------------------
00:02:03:04:05:08  00:02:03:04:05:06
```

```
                    00:02:03:04:05:07
```

show wireless ssid client status

This command displays 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. The SSID/network may exist on one or more managed AP VAPs.

Format **show wireless ssid** *[<ssid>]* **client status**

Mode Privileged EXEC

Field	*Description*
ssid	Service Set Identifier for the network.
MAC Address	The Ethernet address of the client station.
SSID	Indicates the network on which the client is connected.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless ssid client status

                                    Client
             SSID                  MAC Address    Channel    Status
------------------------------ ----------------- ------- --------------------
Network2                       00:01:01:16:01:01 44      Authenticated
                               00:01:01:20:01:01 44      Authenticated
                               00:01:01:22:01:01 44      Authenticated
Network3                       00:01:01:10:01:01 6       Associated
                               00:01:01:14:01:01 6       Authenticated

(DWS-4026) #
```

show wireless switch client status

This command displays summary data for all switches with associated clients. If the Unified Switch is a WIDS 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** *[<ipaddr>]* **client status**

Mode Privileged EXEC

Field	*Description*
ipaddr	IP address of the switch in the wireless system.
IP Address	IP address of the Unified Switch or any peer switch in the wireless system.
MAC Address	The Ethernet address of the client station.

Example: The following shows example CLI display output for the command.

If a network consists of two switches 192.168.37.60 and 192.168.37.61 respectively and former is the Cluster Controller, this command works differently at Cluster Controller and non-Cluster Controller as follows.

On the Cluster Controller, it displays entries in the following format:

```
 (DWS-4026) #show wireless switch client status

                                    Client
       Switch IP Address            MAC Address     Channel       Status
------------------------------ -----------------  ------- --------------------
         192.168.37.60           00.0F.B5.86.93.95    1         Authenticated
                                 00:14:C2:0C:47:6D    1         Authenticated
         192.168.37.61           00.0F.B5.86.93.85    6         Authenticated
                                 00:14:C2:0C:47:1D   11         Authenticated

(DWS-4026) #show wireless switch 192.168.37.60 client status

                                    Client
       Switch IP Address            MAC Address     Channel       Status
------------------------------ -----------------  ------- --------------------
         192.168.37.60           00.0F.B5.86.93.95    1         Authenticated
                                 00:14:C2:0C:47:6D    1         Authenticated

(DWS-4026) #show wireless switch 192.168.37.61 client status

                                    Client
       Switch IP Address            MAC Address     Channel       Status
------------------------------ -----------------  ------- --------------------
         192.168.37.61           00.0F.B5.86.93.85    6         Authenticated
                                 00:14:C2:0C:47:1D   11         Authenticated

On the switch that is not acting as a Cluster Controller the summary command displays
entries in the following format:

(DWS-4026) #show wireless switch client status

                                    Client
       Switch IP Address            MAC Address     Channel       Status
------------------------------ -----------------  ------- --------------------
         192.168.37.61           00.0F.B5.86.93.85    6         Authenticated
                                 00:14:C2:0C:47:1D   11         Authenticated

(DWS-4026) #show wireless switch 192.168.37.60 client status
Error! Only Cluster Controller can display the peer switch associated client status.

(DWS-4026) #show wireless switch 192.168.37.61 client status
                                    Client
       Switch IP Address            MAC Address     Channel       Status
------------------------------ -----------------  ------- --------------------
         192.168.37.61           00.0F.B5.86.93.85    6         Authenticated
                                 00:14:C2:0C:47:1D   11         Authenticated
```

CLIENT FAILURE AND AD HOC STATUS COMMANDS

The commands in this section provide views and management of data maintained for wireless client association and authentication failures.

clear wireless client failure list

This command deletes all entries from the client failure list. Entries normally age out according to the configured age time.

Format	**clear wireless client failure list**
Mode	Privileged EXEC

Example: The following shows an example of the command.

```
(DWS-4026) #clear wireless client failure list
Are you sure you want to clear all client failure entries? (y/n) y
All client failure entries cleared.
```

clear wireless client adhoc list

This command deletes all entries from the Ad Hoc client list. Entries normally age out according to the configured age time.

Format	**clear wireless client adhoc list**
Mode	Privileged EXEC

show wireless client failure status

This command displays the client failure status parameters.

Format	**show wireless client** *[<macaddr>]* **failure status**
Mode	Privileged EXEC

Field	*Description*
macaddr	Client MAC address.
MAC Address	The Ethernet address of the client.
VAP MAC Address	The managed AP VAP Ethernet MAC address on which the client attempted to associate and/or authenticate.
SSID	The network SSID on which the client attempted to associate and/or authenticate.
Last Failure Type	Indicates the last type of failure that occurred.
Authentication Failure Count	Count of authentication failures for this client.
Association Failure Count	Count of association failures for this client.
Age	Time since failure occurred.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless client failure status

                                                                  Failure
   MAC Address     VAP MAC Address           SSID                 Type      Age
---------------- ---------------- ---------------------- ------- -----------
00:01:21:18:01:01 00:01:01:02:02:02 Network2               Auth    0h:1m:38s
00:01:32:18:01:01 00:01:01:02:01:03 Network3               Assoc   0h:1m:44s

(DWS-4026) #
(DWS-4026) #show wireless client 00:01:21:18:01:01 failure status

MAC Address..................................... 00:01:21:18:01:01
VAP MAC Address................................. 00:01:01:02:02:02
SSID............................................ Network2
Last Failure Type............................... Authentication
Association Failure Count....................... 0
Authentication Failure Count.................... 2
Age............................................. 0h:3m:14s

(DWS-4026) #
```

show wireless client adhoc status

This command displays summary or detailed data for Ad Hoc clients detected on the network by a managed AP.

Format **show wireless client** *[<macaddr>]* **adhoc status**

Mode Privileged EXEC

Field	*Description*
macaddr	Client MAC address.
MAC Address	The Ethernet address of the client. If the Detection Mode is Beacon, then the client is represented as an AP in the RF Scan database and the Neighbor AP List. If the Detection Mode is Data Frame, then the client information is in the Neighbor Client List.
AP MAC Address	The base Ethernet MAC Address of the managed AP which detected the client.
Location	The configured descriptive location for the managed AP.
Radio	The radio interface on the AP that detected the ad hoc device.
Detection Mode	The mechanism of detecting this Ad Hoc device. The possible values are *Beacon Frame* or *Data Frame*.
Age	Time in seconds since the last detection of the ad hoc network.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show wireless client adhoc status

   MAC Address     AP MAC Address    Location   Radio Detection Mode     Age
---------------- ---------------- ----------- ----- -------------- ----------
00:01:01:30:01:01 00:01:01:02:01:01 FirstFloor  1     Beacon Frame   3h:45m:4s
00:01:01:42:01:01 00:01:01:02:03:01 Eng         1     Beacon Frame   3h:44m:59s
00:01:01:45:01:01 00:01:01:02:01:01 FirstFloor  1     Beacon Frame   3h:45m:2s
(DWS-4026) #
```

WIDS ACCESS POINT RF SECURITY COMMANDS

The commands in this section provide views and management of data maintained for the Wireless Intrusion Detection System (WIDS) for RF Security.

wids-security admin-config-rogue

(Administrator-configured rogue detection.) If the local database indicates that an AP is rogue, use this command to report the AP as rogue in the RF Scan.

Default	Enable
Format	`wids-security admin-config-rogue`
Mode	Wireless Config

wids-security ap-chan-illegal

(AP is operating on an illegal channel Rogue Detection.) Use this command to enable rogue reporting for AP's operating on an illegal channel.

Default	Enable
Format	`wids-security ap-chan-illegal`
Mode	Wireless Config

no wids-security ap-chan-illegal

Use this command to disable the mode to report APs operating on an illegal channel.

Format	`no wids-security ap-chan-illegal`
Mode	Wireless Config

wids-security ap-de-auth-attack

(AP de-authentication attack.) Use this command to enable the AP de-authentication attack.

Default	Disable
Format	`wids-security ap-de-auth-attack`
Mode	Wireless Config

no wids-security ap-de-auth-attack

Use this command to disable the AP de-authentication attack.

Format	`no wids-security ap-de-auth-attack`
Mode	Wireless Config

wids-security fakeman-ap-managed-ssid

Use this command to enable Rogue reporting for fake managed AP's detected with a managed SSID.

Default	Enable
Format	`wids-security fakeman-ap-managed-ssid`
Mode	Wireless Config

no wids-security fakeman-ap-managed-ssid

Use this command to disable Rogue reporting for fake managed AP's detected with a managed SSID.

Format	`no wids-security fakeman-ap-managed-ssid`
Mode	Wireless Config

wids-security fakeman-ap-chan-invalid

(Beacon received from a fake managed AP on an invalid channel Rogue Detection.) Use this command to enable rogue reporting for fake managed APs detected with an invalid channel.

Default	Enable
Format	`wids-security fakeman-ap-chan-invalid`
Mode	Wireless Config

no wids-security fakeman-ap-chan-invalid

Use this command to disable Rogue reporting for fake managed AP's detected with an invalid channel.

Format	`no wids-security fakeman-ap-chan-invalid`
Mode	Wireless Config

wids-security fakeman-ap-no ssid

(Beacon received from fake managed AP without SSID rogue detection.) Use this command to enable rogue reporting for fake managed AP's detected with no SSID.

Default	Enable
Format	`wids-security fakeman-ap-no-ssid`
Mode	Wireless Config

no wids-security fakeman-ap-no ssid

Use this command to disable rogue reporting for fake managed APs detected with an invalid channel.

Format	`no wids-security fakeman-ap-no ssid`
Mode	Wireless Config

wids-security managed-ap-ssid-invalid

(Invalid SSID received from a managed AP Rogue Detection.) Use this command to enable rogue reporting for managed AP's detected with an invalid SSID.

Default	Enable
Format	**wids-security managed-ap-ssid-invalid**
Mode	Wireless Config

no wids-security managed-ap-ssid-invalid

Use this command to disable the mode to report managed APs detected with an invalid SSID.

Format	**no wids-security managed-ap-ssid-invalid**
Mode	Wireless Config

wids-security managed-ssid-secu-bad

(Managed SSID detected with incorrect security configuration Rogue Detection). Use this command to enable rogue reporting for AP's detected with managed SSID's and an invalid security configuration.

Default	Enable
Format	**wids-security managed-ssid-secu-bad**
Mode	Wireless Config

no wids-security managed-ssid-secu-bad

Use this command to disable the mode to report AP's detected with managed SSID's and an invalid security configuration.

Format	**no wids-security managed-ssid-secu-bad**
Mode	Wireless Config

wids-security rogue-det-trap-interval

(Rogue-detected trap interval.) Use this command to set the interval in seconds between transmissions of the trap telling you that rogues are present in the RF Scan database.

Default	300
Format	**wids-security rogue-det-trap-interval** *<60-3600>*
Mode	Wireless Config

Parameter	*Description*
0, 60-3600	The interval in seconds between transmissions of the trap telling you that rogues are present in the RF Scan database. The trap interval range is 60-3600 seconds. A configured value of 0 disables the trap from being set.

no wids-security rogue-det-trap-interval

Use this command to restore the rogue detected trap interval to its default value.

Format	`no wids-security rogue-det-trap-interval`
Mode	Wireless Config

wids-security standalone-cfg-invalid

(Standalone AP is operating with unexpected channel, SSID, security, or WIDS mode Rogue Detection.) Use this command to enable rogue reporting for standalone APs operating with unexpected channel, SSID, security, or WIDS mode.

Default	Enable
Format	`wids-security standalone-cfg-invalid`
Mode	Wireless Config

no wids-security standalone-cfg-invalid

Use this command to disable the mode to report standalone AP's operating with unexpected channel, SSID, security, or WIDS mode.

Format	`no wids-security standalone-cfg-invalid`
Mode	Wireless Config

wids-security unknown-ap-managed-ssid

(Managed SSID received from unknown AP rogue.) Use this command to enable rogue reporting for unknown rogue APs detected with a managed SSID.

Default	Enable
Format	`wids-security unknown-ap-managed-ssid`
Mode	Wireless Config

no wids-security unknown-ap-managed-ssid

Use this command to disable reporting unknown rogue APs detected with a managed SSID.

Format	`no wids-security unknown-ap-managed-ssid`
Mode	Wireless Config

wids-security unmanaged-ap-wired

(Unmanaged AP is detected on a wired network Rogue Detection.) Use this command to enable rogue reporting for detection of unmanaged AP's on a wired network.

Default	Enable
Format	**wids-security unmanaged-ap-wired**
Mode	Wireless Config

no wids-security unmanaged-ap-wired

Use this command to disable the mode to report unmanaged APs on a wired network.

Format	**no wids-security unmanaged-ap-wired**
Mode	Wireless Config

wids-security wds-device-unexpected

(Unexpected WDS device is detected on the network Rogue Detection.) Use this command to enable rogue reporting for detection of unexpected WDS devices.

Default	Enable
Format	**wids-security wds-device-unexpected**
Mode	Wireless Config

no wids-security wds-device-unexpected

Use this command to disable the mode to report detection of unexpected WDS devices.

Format	**no wids-security wds-device-unexpected**
Mode	Wireless Config

wids-security wired-detection-interval

(Minimum wired detection interval.) Use this command to set the minimum number of seconds that the AP waits before starting a new wired network detection cycle.

Default	60
Format	**wids-security wired-detection-interval** *<interval>*
Mode	Wireless Config

Parameter	*Description*
interval	Minimum number of seconds that the AP waits before starting a new wired network detection cycle. The range is 1-3600 seconds. A value of zero (0) disables wired detection.

no wids-security wired-detection-interval

This command restores the minimum wired detection interval to its default value.

Format `no wids-security wired-detection-interval`

Mode Wireless Config

show wireless wids-security

This command displays the configured wireless WIDS security settings.

Format `show wireless wids-security`

Mode Privileged EXEC

Field	*Description*
Rogue - admin configured Rogue APs	If the local database indicates that the AP is rogue, then reports the AP as rogue in the RF Scan.
Rogue - APs on an illegal channel	Enable or disable rogue reporting for APs operating on an illegal channel.
Rogue - fake managed AP/ invalid channel	Enable or disable rogue reporting for fake managed APs on an invalid channel.
Rogue - fake managed AP/no SSID	Enable or disable rogue reporting for fake managed APs without an SSID.
Rogue - managed AP/invalid SSID	Enable or disable rogue reporting for a managed AP with an invalid SSID.
Rogue - managed SSID/invalid security	Enable or disable rogue reporting for APs with a managed SSID and an incorrect security configuration.
Rogue - standalone AP/unexpected config	Enable or disable rogue reporting for standalone APs operating with unexpected channel, security, or WIDS mode.
Rogue - unknown AP/managed SSID	Enable or disable rogue reporting for unknown rogue APs detected with a managed SSID.
Rogue - unmanaged AP on a wired network	Enable or disable rogue reporting for unmanaged APs on a wired network.
Rogue - unexpected WDS devices	Enable or disable rogue reporting for unexpected WDS devices detected on the network.
Rogue detected trap interval	The interval in seconds between transmissions of the trap telling the administrator that rogues are present in the RF Scan database.
Wired network detection interval	Minimum number of seconds that the AP waits before starting a new wired network detection cycle.
AP De-authentication Attack	Enable or disable the AP De-authentication attack.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) # 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 - unmanaged AP on a wired network..... Enable
Rogue - unexpected WDS devices..... Enable
Rogue detected trap interval..... 60 seconds
Wired network detection interval..... 60 seconds
AP De-Authentication Attack..... Disable
```

show wireless wids-security rogue-classification

This command displays the WIDS AP rogue classification test results.

Format **show wireless wids-security** *<macaddr>* **rogue-classification**

Mode Privileged EXEC

Field	*Description*
macaddr	MAC address of the rogue AP.
TestID	Test identifier (WIDSAPROGUEnn).
Detect	Indicates whether this test detected the condition that it is designed to detect. Possible values are **True** or **False**.
MAC Addr (radio)	The Managed AP MAC address and (radio number) last reported detecting this condition.
Config	Indicates whether this test is configured to report rogues. Possible values are **Enable** or **Disable**.
Result	Indicates whether this test reported the device as rogue (Possible values are **Rogue** or empty string.)
1st Report	Time stamp indicating how long ago this test first detected the condition.
Last Report	Time stamp indicating how long ago this test last detected the condition.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) # show wireless wids-security 00:11:95:A3:7A:C8 rogue-classification

Test ID       Detect   MAC Addr (radio)   Config  Result 1st Report  Last Report
------------- ------ -------------------- ------- ------ ----------- -----------
WIDSAPROGUE01 True   00:00:00:00:00:11(1) Enable  Rogue  0d:00:00:00 0d:00:00:01
WIDSAPROGUE02 False  00:00:00:00:00:12(2) Disable        0d:00:00:00 0d:00:00:00
WIDSAPROGUE03 True   00:00:00:00:00:13(0) Enable  Rogue  0d:00:00:02 0d:00:00:03
WIDSAPROGUE04 True   00:00:00:00:00:14(1) Enable  Rogue  0d:00:00:04 0d:00:00:05
WIDSAPROGUE05 True   00:00:00:00:00:15(2) Enable  Rogue  0d:00:00:06 0d:00:00:07
WIDSAPROGUE06 True   00:00:00:00:00:16(0) Enable  Rogue  0d:00:01:28 0d:00:01:39
WIDSAPROGUE07 False  00:00:00:00:00:17(1) Enable         0d:00:01:51 0d:00:03:42
WIDSAPROGUE08 False  00:00:00:00:00:18(2) Enable         0d:00:05:33 0d:00:07:24
WIDSAPROGUE09 False  00:00:00:00:00:19(2) Enable         0d:00:09:15 0d:00:11:06
WIDSAPROGUE10 False  00:00:00:00:00:1A(0) Enable         0d:00:12:57 0d:00:14:48

To see test descriptions use show wireless wids-security rogue-test-descriptions.
```


show wireless wids-security rogue-test-descriptions

This command displays the WIDS AP rogue classification test identifier descriptions.

Format **show wireless wids-security rogue-test-descriptions**
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) # 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
```

show wireless wids-security de-authentication

This command displays information about APs against which the Cluster Controller initiated a de-authentication attack.

Format **show wireless wids-security de-authentication**
Mode Privileged EXEC

Field	*Description*
BSSID	BSSID of the AP against which the attack is launched.
Channel	Channel on which the rogue AP is operating.
Attack Time	Time since attack started on this AP.
Age	Time since RF Scan report about this AP.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) # 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
00:02:BB:00:32:05   15    0d:00:09:15 0d:00:07:20
00:02:BB:00:3C:06   18    0d:00:11:06 0d:00:08:48
00:02:BB:00:46:07   21    0d:00:12:57 0d:00:10:16
00:02:BB:00:50:08   24    0d:00:14:48 0d:00:11:44
00:02:BB:00:5A:09   27    0d:00:16:39 0d:00:13:12
```

```
00:02:BB:00:64:0A   30    0d:00:18:30 0d:00:14:40
00:02:BB:00:6E:0B   33    0d:00:20:21 0d:00:16:08
00:02:BB:00:78:0C   36    0d:00:22:12 0d:00:17:36
00:02:BB:00:82:0D   39    0d:00:24:03 0d:00:19:04
00:02:BB:00:8C:0E   42    0d:00:25:54 0d:00:20:32
00:02:BB:00:96:0F   45    0d:00:27:45 0d:00:22:00
00:02:BB:00:A0:10   48    0d:00:29:36 0d:00:23:28
```


DETECTED CLIENTS DATABASE COMMANDS

This section provides status and configuration commands for the detected client database.

wids-security client rogue-det-trap-interval

Use this command to set the interval in seconds between transmissions of the trap telling you that rogue clients are present in the Detected Clients Database.

Default 60

Format **wids-security client rogue-det-trap-interval** *<0-3600>*

Mode Wireless Config

Parameter	*Description*
0-3600	Interval in seconds between transmissions of the trap. The range is 0-3600 seconds. A configured value of 0 disables the trap from being sent.

no wids-security client rogue-det-trap-interval

Use this command to restore the rogue detection trap interval to its default value, 60.

Format **no wids-security client rogue-det-trap-interval**

Mode Wireless Config

Example: The following shows an example of the command.

```
(DWS-4026) # wids-security client rogue-det-trap-interval 60  ?
<cr>   Press Enter to execute the command.

(DWS-4026) # no wids-security client rogue-det-trap-interval ?
<cr>   Press Enter to execute the command.
```

wids-security client known-client-database

Use this command to enable the test which marks the client as a rogue if it is not in the Known Clients database.

Default Disable

Format **wids-security client known-client-database**

Mode Wireless Config

no wids-security client known-client-database

Use this command to disable the check for the client in the Known Clients database.

Format **no wids-security client known-client-database**

Mode Wireless Config

wids-security client configured-auth-rate

Use this command to enable the test which marks the client as rogue if it exceeds the configured rate for transmitting 802.11 authentication requests.

Default	Enable
Format	`wids-security client configured-auth-rate`
Mode	Wireless Config

no wids-security client configured-auth-rate

Use this command to disable the test for checking if the client exceeds the configured rate for transmitting 802.11 authentication requests.

Format	`no wids-security client configured-auth-rate`
Mode	Wireless Config

wids-security client configured-probe-rate

Use this command to enable the test which marks the client as rogue if it exceeds the configured rate for transmitting probe requests.

Default	Enable
Format	`wids-security client configured-probe-rate`
Mode	Wireless Config

no wids-security client configured-probe-rate

Use this command to disable the test for checking if the client exceeds the configured rate for transmitting probe requests.

Format	`no wids-security client configured-probe-rate`
Mode	Wireless Config

wids-security client configured-deauth-rate

Use this command to enable the test which marks the client as rogue if it exceeds the configured rate for transmitting 802.11 de-authentication requests.

Default	Enable
Format	`wids-security client configured-deauth-rate`
Mode	Wireless Config

no wids-security client configured-deauth-rate

Use this command to disable the test for checking if the client exceeds the configured rate for transmitting 802.11 de-authentication requests.

Format `no wids-security client configured-deauth-rate`
Mode Wireless Config

wids-security client max-auth-failure

Use this command to enable the test which marks the client as rogue if it exceeds the maximum number of authentication failures.

Default Enable
Format `wids-security client max-auth-failure`
Mode Wireless Config

no wids-security client max-auth-failure

Use this command to disable the test for checking if the client has exceeded the configured rate for maximum authentication failures.

Format `no wids-security client max-auth-failure`
Mode Wireless Config

wids-security client auth-with-unknown-ap

Use this command to enable the test to check if a known client is authenticated with an unknown AP. If yes, then the client is marked as a rogue.

Default Enable
Format `wids-security client auth-with-unknown-ap`
Mode Wireless Config

no wids-security client auth-with-unknown-ap

Use this command to disable the test for checking if the client is authenticated with an unknown AP.

Format `no wids-security client auth-with-unknown-ap`
Mode Wireless Config

wids-security client threat-mitigation

Use this command to enable the transmission of de-authentication messages to known clients associated with unknown APs. The “Known Client” test must also be enabled order for the mitigation to take place.

Default Disable
Format `wids-security client threat-mitigation`
Mode Wireless Config

no wids-security client threat-mitigation

Use this command to disable the test for Client Threat Mitigation.

Format	**no wids-security client threat-mitigation**
Mode	Wireless Config

wids-security client threshold-value-deauth

Use this command to configure the maximum number of de-authentication messages which a switch can receive during the threshold interval.

Default	10
Format	**wids-security client threshold-value-deauth** *<1-99999>*
Mode	Wireless Config

Parameter	*Description*
1-99999	Range of the threshold value.

no wids-security client threshold-value-deauth

Use this command to set the threshold-value for de-authentication messages to the default.

Format	**no wids-security client threshold-value-deauth**
Mode	Wireless Config

wids-security client threshold-interval-deauth

Use this command to configure the threshold interval for counting the de-authentication messages.

Default	60
Format	**wids-security client threshold-interval-deauth** *<1-3600>*
Mode	Wireless Config

Parameter	*Description*
1-3600	Range of the threshold value.

no wids-security client threshold-interval-deauth

Use this command to set the threshold value for the de-authentication interval to its default.

Format	**no wids-security client threshold-interval-deauth**
Mode	Wireless Config

wids-security client threshold-value-auth

Use this command to configure the maximum number of authentication messages a switch can receive during the threshold interval.

Default 10
Format **wids-security client threshold-value-auth** *<1-99999>*
Mode Wireless Config

Parameter	*Description*
1-99999	The range of the threshold value.

no wids-security client threshold-value-auth

Use this command to set the threshold value for authentication messages to its default.

Format **no wids-security client threshold-value-auth**
Mode Wireless Config

wids-security client threshold-interval-auth

Use this command to configure the threshold interval for counting the authentication messages at the switch.

Default 60
Format **wids-security client threshold-interval-auth** *<1-3600>*
Mode Wireless Config

no wids-security client threshold-interval-auth

Use this command to set the threshold value for the authentication interval to its default.

Format **no wids-security client threshold-interval-auth**
Mode Wireless Config

wids-security client threshold-value-probe

Use this command to configure the maximum number of probe messages a switch can receive during the threshold interval.

Default 120
Format **wids-security client threshold-value-probe** *<1-99999>*
Mode Wireless Config

Parameter	*Description*
1-99999	The range of the threshold value.

no wids-security client threshold-value-probe

Use this command to set the threshold value for probe messages to the default.

Format `no wids-security client threshold-value-probe`
Mode Wireless Config

wids-security client threshold-interval-probe

Use this command to configure the threshold interval for counting the probe messages.

Default 60
Format `wids-security client threshold-interval-probe <1-3600>`
Mode Wireless Config

Parameter	*Description*
1-3600	The range of the threshold value.

no wids-security client threshold-interval-probe

Use this command to set the threshold value for the probe interval to its default.

Format `no wids-security client threshold-interval-probe`
Mode Wireless Config

wids-security client threshold-auth-failure

Use this command to configure the number of 802.1X authentication failures that triggers the client to be reported as rogue.

Default 5
Format `wids-security client threshold-auth-failure <1-99999>`
Mode Wireless Config

Parameter	*Description*
1-99999	The range of the threshold value.

no wids-security client threshold-auth-failure

Use this command to set the threshold value for authentication failures to its default.

Format `no wids-security client threshold-auth-failure`
Mode Wireless Config

wids-security client known-db-location

Use this command to configure the location of the Known-Client database for detected clients.

Default Local
Format **wids-security client known-db-location** *<local | radius-server>*
Mode Wireless Config

Parameter	*Description*
local	Database defined locally.
radius-server	Database defined on a radius-server.

no wids-security client known-db-location

Use this command to set the location of the Known-Client database for detected clients to the default.

Format **no wids-security client known-db-location**
Mode Wireless Config

wids-security client known-db-radius-server-name

Use this command to configure the radius-server name of the Known-Client database for detected clients.

Default Default-RADIUS-Server
Format **wids-security client known-db-radius-server-name** *<name>*
Mode Wireless Config

Parameter	*Description*
name	An alphanumeric string up to 32 characters in length.

no wids-security client known-db-radius-server-name

Use this command to set the Known-Client database radius-server name for detected clients to the default.

Format **no wids-security client known-db-radius-server-name**
Mode Wireless Config

detected-client ack-rogue

Use this command to change the client status from Rogue to Known or Authenticated for the specified client MAC address. If no client is specified, the command changes the client status for all of the clients.

Format **detected-client** *[<macaddr>]* **ack-rogue**
Mode Wireless Config

Parameter	*Description*
macaddr	The Ethernet address of the client.

clear wireless detected-client list

Use this command to delete the client entry for the specified MAC address or all the entries present in the database. If the client is authenticated, then this command has no effect.

Format **clear wireless** *[<macaddr>]* **detected-client**

Mode Privileged EXEC

Parameter	*Description*
macaddr	The Ethernet address of the client.

Example: The following shows an example of the command.

```
clear wireless detected-client list
Are you sure you want to clear all the wireless detected clients? (y/n)y
Wireless detected-client list cleared.
```

show wireless client detected-client preauth-history

Use this command to display the pre-authentication events that have occurred for the specified client or for all the clients present 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.

Format **show wireless client** *[<macaddr>]* **detected-client preauth-history**

Mode Privileged EXEC

Field	*Description*
Mac Address	The Ethernet address of the client.
AP Mac Address	The Ethernet address of the Access Point with which the client is pre-authenticated.
Radio	The radio interface on the AP.
VAP Mac Address	The Ethernet address of the VAP to which client has roamed.
SSID	The RF Noise perceived by the reporting AP for the specified detected client.
Pre-Auth Status	Indicates whether the client is successfully pre-authenticated.
Time Since Event	Time since entry was last updated.

show wireless client detected-client roam-history

Use this command to display the roaming history for the specified MAC address or all the clients in the detected client database. A roaming history of up to ten Access Points is displayed, as only the maximum of ten records are maintained for each client. Clients that never authenticated with the managed network do not display in the list.

Format **show wireless client** *<macaddr>* **detected-client roam-history**

Mode Privileged EXEC

Field	*Description*
Mac Address	The Ethernet address of the client.
AP Mac Address (Radio)	The Ethernet address of the Access Point with which the client is pre-authenticated.
Radio	The radio interface on the AP.
VAP Mac Address	The Ethernet address of the VAP to which client has roamed.
SSID	The RF Noise perceived by the reporting AP for the specified detected client.
Auth Status	Shows if the client authentication was due to new authentication or roaming.
Time Since Roam	Time since entry was last updated.

show wireless client detected-client rogue-classification

Use this command to display the WIDS rogue classification test results for a particular client MAC address.

Format **show wireless client** *<macaddr>* **detected-client rogue-classification**

Mode Privileged EXEC

Field	*Description*
macaddr	The client MAC address.
Test ID	Test identifier (WIDSCLNTROGUEnn).
Detect	Indicates whether this test detected the condition that it is designed to detect. Valid values are **no detection** or **Condition Detected**.
MAC Addr (radio)	The Managed AP MAC address and (radio number) that last reported detecting this condition.
Config	Indicates whether this test is configured to report rogues. Valid values are **Enable** or **Disable**.
Result	Indicates whether this test reported the device as rogue. Valid values are **Rogue** or empty string.
1st Report	Time stamp indicating how long ago this test first detected the condition.
Last Report	Time stamp indicating how long ago this test last detected the condition.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) # show wireless client 00:02:BB:00:14:02 detected-client rogue-classification
WIDSCLNTROGUE1.............................. Client not in Known Client Database
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
```

show wireless client detected-client status

Use this command to display status information for detected clients. If you do not enter a parameter, the command displays summary status for all detected clients in the database. if you enter a client MAC address, the command displays detailed status for that detected client.

Format `show wireless client <macaddr> detected-client status`

Mode Privileged EXEC

Field	*Description*
MAC Address	The Ethernet address of the client.
OUI	The organizationally unique identifier for the wireless client.
Client Status	The detected client status.
Auth Status	Shows whether the client is authenticated or not.
Time Since Last Updated	Time since entry was last updated.
Threat Detection	Shows if the threat detection test is triggered for this client.
Threat Mitigation	Shows if threat mitigation has been done for this client.
Client Name	Shows the name of the client.
Time Since Created	Time since entry was created.
Channel	Channel in which the client is detected.
Auth RSSI	RSSI reported by the managed AP with which the client is authenticated.
Auth Signal	Signal strength reported by the managed AP with which the client is authenticated.
Auth Noise	Noise reported by the managed AP with which the client is authenticated.
Probe Req	Number of probe requests during the collection interval.
Probe Collection Interval	The time remaining in the probe collection interval.
Highest Num Probes	The largest number of probes that the switch detected during the collection interval.
Auth Req	The number of 802.11 authentication messages recorded so far during the probe collection interval.
Auth Collection Interval	The amount of time left before the authentication collection interval is done and the switch decides whether the client is a threat.
Highest Num Auth Msgs	The largest number of authentications that the switch detected during the collection interval.
DeAuth Req	The number of 802.11 de-authentication messages recorded so far during the probe collection interval.
DeAuth Collection Interval	The amount of time left before the de-authentication collection interval is done and the switch decides whether the client is a threat.
Highest Num DeAuth Msgs	The largest number of de-authentications that the switch detected during the collection interval.
Num Auth Failures	The number of 802.1X authentication failures detected for this client.
Total Probe Messages	The number of probes detected in the last RF Scan.
Broadcast BSSID Probes	The number of probes to broadcast BSSID in the last RF Scan.

Field	*Description*
Broadcast SSID Probes	The number of probes to Broadcast SSID in the last RF Scan.
Specific BSSID Probes	The number of probes to Specific BSSID in the last RF Scan.
Specific SSID Probes	The number of probes to Specific SSID in the last RF Scan.
Last Non-Broadcast BSSID	The last non-broadcast BSSID detected in the RF Scan.
Last Non-Broadcast SSID	The last non-broadcast SSID detected in the RF Scan.
Threat Mitigation Sent	The time since the switch sent the last threat mitigation message to this client.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) # show wireless client detected-client status
Mac Address         Client Name    Client Status       Age           Create Time
--------------------------------------------------------------------------------
00:02:BB:00:0A:01   TestClient1    Known               0d:00:01:51    0d:00:01:10
00:02:BB:00:14:02   TestClient2    Rogue               0d:00:14:40    0d:00:14:30

(DWS-4026) # show wireless client 00:13:46:C1:78:67 detected-client status
MAC address..................................... 00:13:46:C1:78:67
OUI............................................. D-Link Corporation
Client Status................................... Authenticated
Auth Status..................................... Authenticated
Time Since Last Updated......................... 0d:00:00:02
Threat Detection................................ Detected
Threat Mitigation............................... Not Done
Client Name.....................................
Time Since Created.............................. 0d:02:17:19
Channel......................................... 6
Auth RSSI....................................... 14
Auth Signal..................................... -81
Auth Noise...................................... -89
Probe Req....................................... 12
Probe Collection Interval....................... 0d:00:00:41
Highest Num Probes.............................. 10
Auth Req........................................ 0
Auth Collection Interval........................ 0d:00:00:41
Highest Num Auth Msgs........................... 0
DeAuth Req...................................... 0
DeAuth Collection Interval...................... 0d:00:00:41
Highest Num DeAuth Msgs......................... 0
Num Auth Failures............................... 0
Total Probe Msgs................................ 20
Broadcast BSSID Probes.......................... 10
Broadcast SSID Probes........................... 10
Specific BSSID Probes........................... 0
Specific SSID Probes............................ 0
Last Non-Broadcast BSSID........................ 00:00:00:00:00:00
Last Non-Broadcast SSID.........................
Threat Mitigation Sent.......................... 0d:00:00:00
```

show wireless client detected-client triangulation

Use this command to display the signal triangulation status for the specified client entry.

Format `show wireless client <macaddr> detected-client triangulation`

Mode Privileged EXEC

Field	*Description*
AP Function	Indicates whether the reporting AP is operating in Sentry Mode.
AP Mac Address	The Ethernet address of the AP.
RSSI	The RSSI value of received signal for the client at the reporting AP.
Signal	The RF signal strength perceived by the reporting AP in dBm for the specified detected-client.
Noise	The RF Noise perceived by the reporting AP for the specified detected-client.
Detected Time	Time in seconds since the particular AP detected the signal.

show wireless wids-security client

Use this command to display the configured wireless WIDS security settings for the client.

Format `show wireless wids-security client`

Mode Privileged EXEC

Field	*Description*
Rogue Detected Trap Interval	Interval, in seconds, between transmissions of the SNMP trap that indicates the administrator that rogue APs are present in the RF Scan database. If set to 0, the trap is never sent.
Rogue-Not in Known Client List	If client MAC address is not in the Known Client database, then report the client as Rogue.
Rogue-Exceeds Auth Req	If the client exceeds the configured rate for transmitting 802.11 authentication requests, report the client as Rogue.
Rogue-Exceeds DeAuth Reg	If the client exceeds the configured rate for transmitting 802.11 de-authentication requests, report the client as Rogue.
Rogue-Exceeds Probe Req	If the client exceeds the configured rate for transmitting probe requests, report the client as Rogue.
Rogue-Exceeds Failed Auth	If the client exceeds the maximum number of failing authentications, report the client as Rogue.
Rogue-Auth Unknown AP	If the Known Client is authenticated with an Unknown AP, report the client as Rogue.
Client Threat-Mitigation	Indicates whether Client Threat Mitigation is enabled or not.
De-auth Threshold Interval	The number of seconds for counting the de-authentication messages.
De-auth Threshold Value	The maximum number of de-authentication messages the client can send without being reported as rogue.
Auth Threshold Interval	The number of seconds for counting the authentication messages.

Field	*Description*
Auth Threshold Value	The maximum number of authentication messages the client can send without being reported as rogue.
Probe Threshold Interval	The number of seconds for counting the probe messages.
Probe Threshold Value	The maximum number of probe messages the client can send without being reported as rogue.
Auth Failure Threshold	The maximum number of authentication failures that triggers the client to be reported as rogue.
Known DB Location	The location of the Known-Client database for detected clients.
Known DB Radius Server Name	The name of the radius-server for the Known-Client database, defined for detected clients.
Known DB Radius Server Status	Indicates whether or not a radius server for the Known-Client database is configured.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) # show wireless wids-security client
Rogue detected trap interval..................... 300 seconds
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
Known DB Radius Server Name...................... Default-RADIUS-Server
Known DB Radius Server Status.................... Not Configured
```

show wireless wids-security client rogue-test-descriptions

Use this command to display the WIDS Client rogue classification test identifier descriptions.

Format **show wireless wids-security client rogue-test-descriptions**

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) # show wireless wids-security client rogue-test-descriptions

WIDSCLIENTROGUE01.........Client not listed in the Known Clients database
WIDSCLIENTROGUE02.........Client exceeds configured rate for transmitting 802.11
                          authentication requests
WIDSCLIENTROGUE03.........Client exceeds configured rate for transmitting probe requests
```

```
WIDSCLIENTROGUE04.........Client exceeds configured rate for transmitting de-
                          authentication requests
WIDSCLIENTROGUE05.........Client exceeds max num of failing authentications
WIDSCLIENTROGUE06.........Known Client is authenticated with an Unknown AP
```


Section 6: Captive Portal Commands

This section describes the CLI commands you use to manage the Captive Portal features on the switch.

This section contains the following subsections:

Captive Portal Global Commands

The commands in this section enable you to configure the captive portal settings that affect the captive portal feature on the switch and all captive portal instances.

captive-portal

Use this command to enter the Captive Portal Configuration Mode.

Format	`captive-portal`
Mode	Global Config

enable (Captive Portal Config Mode)

This command globally enables the captive portal feature on the switch.

Default	Disable
Format	`enable`
Mode	Captive Portal Config

no enable (Captive Portal Config Mode)

The `no` version of this command disables the captive portal functionality.

Format	`no enable`
Mode	Captive Portal Config

http port

This command configures an additional HTTP port. Valid port numbers are in the range of 0-65535, excluding port numbers 80 and 443 which are reserved. The HTTP port default is 0 which denotes no additional port and the default port (80) is used.

Default	0
Format	**http port** *<port-num>*
Mode	Captive Portal Config

Example: The following shows an example of the command.

```
(DWS-4026) (Config-CP) #http port 8080<cr>
(DWS-4026) (Config-CP) #no http port<cr>
```

no http port

This command removes the specified additional HTTP port.

Format	**no http port** *<port-num>*
Mode	Captive Portal Config

https port

This command configures an additional HTTPS secure port. The HTTPS secure port default is 0 which denotes no additional port and the default port (443) is used.

Default	0
Format	**https port** *<port-num>*
Mode	Captive Portal Config

Parameter	*Description*
port-num	Port number in the range of 0-65535.

Example: The following shows an example of the command.

```
(DWS-4026) (Config-CP) #https port 60000<cr>
(DWS-4026) (Config-CP) #no https port<cr>
```

no https port

This command set the HTTPS secure port to the default.

Format	**no https port** *<port-num>*
Mode	Captive Portal Config

statistics interval

Use this command to configure the interval at which statistics are reported in the Cluster Controller. The reporting interval is in the range of 0, 15-3600 seconds where 0 disables statistical reporting.

Default	120
Format	**statistics interval** *<interval>*
Mode	Captive Portal Config

no statistics interval

Use this command to set the reporting interval to the default.

Format	**no statistics interval**
Mode	Captive Portal Config

snmp-server enable traps captive-portal

This command globally enables the captive portal traps. The specific captive portal traps are configured using the **trapflags** command in Captive Portal Config Mode.

Default	Disable
Format	**snmp-server enable traps captive-portal**
Mode	Global Config

no snmp-server enable traps captive-portal

This command globally disables all the captive portal traps.

Format	**no snmp-server enable traps captive-portal**
Mode	Global Config

trapflags (Captive Portal Config Mode)

This command enables captive portal SNMP traps. If no parameters are specified, then all traps are enabled. SNMP traps can also be enabled individually by supplying the optional parameters.

The *client-auth-failure* option allows the SNMP agent to send a trap when a client attempts to authenticate with a captive portal but is unsuccessful.

The *client-connect* option allows the SNMP agent to send a trap when a client authenticates with and connects to a captive portal.

The *client-db-full* option allows the SNMP agent to send a trap each time an entry cannot be added to the client database because it is full.

The *client-disconnect* option allows the SNMP agent to send a trap when a client disconnects from a captive portal.

Default	Disabled
Format	**trapflags** *[{client-auth-failure | client-connect | client-db-full | client-disconnect}]*
Mode	Captive Portal Config

no trapflags

This command disables all captive portal SNMP traps when no parameters are specified. The optional parameters specify individual traps to disable.

Format	**no trapflags** *[{client-auth-failure | client-connect | client-db-full | client-disconnect}]*
Mode	Captive Portal Config

authentication timeout

This command configures the authentication timeout. If the captive portal user does not enter valid credentials within this time limit, the authentication page needs to be served again in order for the client to gain access to the network. The *<timeout>* variable is the authentication timeout and is a number in the range of 60-600 seconds.

Default	300
Format	**authentication timeout** *<timeout>*
Mode	Captive Portal Config

no authentication timeout

This command sets the authentication timeout to the default value.

Format	**no authentication timeout**
Mode	Captive Portal Config

show captive-portal

This command reports status of the captive portal feature.

Format	**show captive-portal**
Mode	Privileged EXEC

Field	*Description*
Administrative Mode	Shows whether the CP is enabled.
Operational Status	Indicates whether the CP operational status is enabled or disabled.
Disable Reason	If CP is disabled, this field displays the reason, which can be None, Administratively Disabled, No IPv4 Address, or Routing Enabled, but no IPv4 routing interface.
Captive Portal IP Address	Shows the IP address that the captive portal feature uses.

show captive-portal status

This command reports status of all captive portal instances in the system.

Format `show captive-portal status`

Mode Privileged EXEC

Field	*Description*
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 statistics are reported in 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.
Supported Captive Portals	Shows the number of supported captive portals in the system.
Configured Captive Portals	Shows the number of captive portals configured on the switch.
Active Captive Portals	Shows the number of captive portal instances that are operationally enabled.
Local Supported Users	Shows the number of users that can be added and configured using the local user database.
Configured Local Users	Shows the number of users that are configured from the local user database.
System Supported Users	Shows the total number of authenticated users that the system can support.
Authenticated Users	Shows the number of users currently authenticated to all captive portal instances on this switch.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show captive-portal status
Additional HTTP Port.......................... 0
Additional HTTP Secure Port................... 0
Peer Switch Statistics Reporting Interval..... 120
Authentication Timeout........................ 300
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
```

show captive-portal trapflags

This command shows which captive portal SNMP traps are enabled.

Note: The existing Unified Switch `show trapflags` command shows the global captive portal traps configuration. For more information, see “show trapflags” on page 503. For information about the global settings for the captive portal SNMP traps, see “statistics interval” on page 346.

Format `show captive-portal trapflags`

Mode Privileged EXEC

Field	*Description*
Client Authentication Failure Traps	Shows whether the SNMP agent sends a trap when a client attempts to authenticate with a captive portal but is unsuccessful.
Client Connection Traps	Shows whether the SNMP agent sends a trap when a client authenticates with and connects to a captive portal.
Client Database Full Traps	Shows 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	Shows whether the SNMP agent sends a trap when a client disconnects from a captive portal.

CAPTIVE PORTAL CONFIGURATION COMMANDS

The commands in this section are related to captive portal configurations.

configuration (Captive Portal)

Use this command to enter the Captive Portal Instance Mode.

The captive portal configuration, identified by CP ID 1, is the default CP configuration. You can create up to nine additional captive portal configurations. The system supports a total of ten CP configurations. The Captive Portal ID *<cp-id>* variable is a number in the range of 1-10.

Format	**configuration** *<cp-id>*
Mode	Captive Portal Config

no configuration

This command deletes a captive portal configuration. The command fails if interfaces are associated to this configuration. The default captive portal configuration cannot be deleted. The Captive Portal ID *<cp-id>* variable is a number in the range of 1-10.

Format	**no configuration** *<cp-id>*
Mode	Captive Portal Config

enable (Captive Portal)

This command enables a captive portal configuration.

Default	Enable
Format	enable
Mode	Captive Portal Instance

no enable

This command disables a captive portal configuration.

Format	**no enable**
Mode	Captive Portal Instance

name

This command configures the name for a captive portal configuration. The name can contain up to 32 alphanumeric characters.

Format	**name** *<cp-name>*
Mode	Captive Portal Instance

protocol

This command configures the protocol mode for a captive portal configuration. The CP can use HTTP or HTTPS protocols.

Default	https
Format	**protocol** *{http | https}*
Mode	Captive Portal Instance

verification

This command configures the verification mode for a captive portal configuration. The type of user verification to perform can be one of the following:

- Guest: The user does not need to be authenticated by a database.
- Local: The switch uses a local database to authenticated users.
- RADIUS: The switch uses a database on a remote RADIUS server to authenticate users.

Default	guest
Format	**verification** *{guest | local | radius}*
Mode	Captive Portal Instance

group

This command assigns a group ID to a captive portal configuration. Each Captive Portal configuration must contain at least one group ID. The `group-ID` has a 1-1024 range. Group ID 1 is the default.

Default	group-ID 1
Format	**group** *<group-ID>*
Mode	Captive Portal Instance

radius-accounting

This command enables accounting for a captive portal configuration.

Default	Disable
Format	**radius accounting**
Mode	Captive Portal Instance

no radius-auth-server

This command disables accounting for a captive portal configuration.

Format	**no radius accounting**
Mode	Captive Portal Instance

radius-auth-server

Use this command to configure a captive portal configuration RADIUS authentication server.

Default	Disable
Format	**radius-auth-server** *<server-name>*
Mode	Captive Portal Instance

no radius-auth-server

This command disables a captive portal configuration RADIUS authentication server.

Format	**no radius-auth-server**
Mode	Captive Portal Instance

redirect-url mode

This command enables the redirect mode for a captive portal configuration.

Default	Disable
Format	**redirect-url mode**
Mode	Captive Portal Instance

no redirect-url mode

This command disables the redirect mode for a captive portal configuration.

Format	**no redirect-url mode**
Mode	Captive Portal Instance

redirect-url

Use this command to specify the URL to which the newly authenticated client is redirected if the URL Redirect Mode is enabled. This command is only available if the redirect mode is enabled.

Format	**redirect-url** *<url>*
Mode	Captive Portal Instance

max-bandwidth-up

This command configures the maximum rate at which a client can send data into the network.

no max-bandwidth-up

Default 0

Format **max-bandwidth-up** *<rate>*

Mode Captive Portal Config

Parameter	*Description*
rate	Rate in bps. 0 indicates limit not enforced.

This command sets to the default the maximum rate at which a client can send data into the network.

Format **no max-bandwidth-up**

Mode Captive Portal Instance

max-bandwidth-down

This command configures the maximum rate at which a client can receive data from the network.

Default 0

Format **max-bandwidth-down** *<rate>*

Mode Captive Portal Instance

Parameter	*Description*
rate	Rate in bps. 0 indicates limit not enforced.

no max-bandwidth-down

This command sets to the default the maximum rate at which a client can receive data from the network.

Format **no max-bandwidth-down**

Mode Captive Portal Instance

max-input-octets

This command configures the maximum number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected. If the value is set to 0 then the limit is not enforced.

Default 0

Format **max-input-octets** *<bytes>*

Mode Captive Portal Instance

Parameter	*Description*
bytes	Input octets in bytes. 0 indicates limit not enforced.

no max-input-octets

This command sets to the default the maximum number of octets the user is allowed to transmit.

Format	`no max-input-octets`
Mode	Captive Portal Instance

max-output-octets

This command configures the maximum number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected. If the value is set to 0 then the limit is not enforced.

Default	0
Format	`max-output-octets` *<bytes>*
Mode	Captive Portal Instance

Parameter	*Description*
bytes	Output octets in bytes. 0 indicates limit not enforced.

no max-output-octets

This command sets to the default the maximum number of octets the user is allowed to receive.

Format	`no max-output-octets`
Mode	Captive Portal Instance

max-total-octets

This command configures the maximum number of octets the user is allowed to transfer, i.e., the sum of octets transmitted and received. After this limit has been reached the user will be disconnected. If the value is set to 0, then the limit is not enforced.

Default	0
Format	`max-total-octets` *<bytes>*
Mode	Captive Portal Instance

Parameter	*Description*
bytes	Total octets in bytes. 0 indicates limit not enforced.

no max-total-octets

This command sets to the default the maximum number of octets the user is allowed to transfer, i.e., the sum of octets transmitted and received.

Format `no max-total-octets`
Mode Captive Portal Instance

session-timeout

This command configures the session timeout for a captive portal configuration. The *<timeout>* variable is a number that represents the session timeout in seconds. Use 0 to indicate that the timeout is not enforced.

Default 0
Format `session-timeout` *<timeout>*
Mode Captive Portal Instance

no session-timeout

Use this command to set the session timeout for a captive portal configuration to the default value.

Format `no session-timeout`
Mode Captive Portal Instance

idle-timeout

This command configures the idle timeout for a captive portal configuration. The *<timeout>* variable is a number that represents the idle timeout in seconds. Use 0 to indicate that the timeout is not enforced.

Default 0
Format `idle-timeout` *<timeout>*
Mode Captive Portal Instance

no idle-timeout

Use this command to set the idle timeout for a captive portal configuration to the default value.

Format `no idle-timeout`
Mode Captive Portal Instance

locale

This command is not intended to be a user command. The administrator must use the WEB user interface to create and customize captive portal web content. The command is primarily used by the Unified Switch `show running config` command and process as it provides the ability to save and restore configurations using a text-based format.

Format `locale` *<web-id>*
Mode Captive Portal Instance

interface

This command associates an interface to a captive portal configuration or removes the interface captive portal association.

Format **interface** *<slot/port>*
Mode Captive Portal Instance

no interface

This command removes the association between an interface and a captive portal configuration.

Format **no interface** *<slot/port>*
Mode Captive Portal Instance

block

This command blocks all traffic for a captive portal configuration.

Format **block**
Mode Captive Portal Instance

no block

This command unblocks all traffic for a captive portal configuration.

Format **no block**
Mode Captive Portal Instance

clear (Captive Portal Instance Config Mode)

This command sets the configuration for this instance to the default values.

Format **clear**
Mode Captive Portal Instance

user-logout

This command enables the ability for an authenticated user to de-authenticate from the network. This command is configurable for a captive portal configuration.

Format **user-logout**
Mode Captive Portal Instance

no user-logout

This command removes the association between an interface and a captive portal configuration.

Format **no user-logout**
Mode Captive Portal Instance

background-color

Use this command to customize the background color of the Captive Portal authentication page using a well-known color name or RGB value. For example, red or RGB hex-code, i.e. #FF0000.The range of *<color-code>* is 1-32 characters.

Default	#BFBFBF
Format	**background-color** *<color-code>*
Mode	Captive Portal Instance

foreground-color

Use this command to customize the foreground color of the Captive Portal authentication page using a well-known color name or RGB value. For example, red or RGB hex-code, i.e. #FF0000.The range of *<color-code>* is 1-32 characters.

Default	#999999
Format	**foreground-color** *<color-code>*
Mode	Captive Portal Instance

separator-color

Use this command to customize the separator bar color of the Captive Portal authentication page using a well-known color name or RGB value. For example, red or RGB hex-code; i.e. #FF0000.The range of *<color-code>* is 1-32 characters.

Default	#BFBFBF
Format	**separator-color** *<color-code>*
Mode	Captive Portal Instance

CAPTIVE PORTAL STATUS COMMANDS

Use the commands in this section to view information about the status of one or more captive portal instances.

show captive-portal configuration

This command displays the operational status of each captive portal configuration. The *<cp-id>* variable is the captive portal ID, which ranges from 1-10.

Format **show captive-portal configuration** *<cp-id>*

Mode Privileged EXEC

Field	*Description*
CP ID	Shows the captive portal ID.
CP Name	Shows the captive portal name.
Operational Status	Shows whether the captive portal is enabled or disabled.
Disable Reason	If the captive portal is disabled, this field indicates the reason.
Blocked Status	Shows the blocked status, which is Blocked or Not Blocked.
Authenticated Users	Shows the number of authenticated users connected to the network through this captive portal.
Configured Locales	Shows the number of locales defined for this captive portal.

show captive-portal configuration interface

This command displays information for all interfaces assigned to a captive portal configuration or a specific interface assigned to a captive portal configuration.

Format **show captive-portal configuration** *<cp-id>* **interface** *[interface]*

Mode Privileged EXEC

Field	*Description*
CP ID	Shows the captive portal ID.
CP Name	Shows the captive portal name.
Interface	Valid slot and port number separated by a forward slash.
Interface Description	Describes the interface.
Operational Status	Shows whether the captive portal is enabled or disabled
Block Status	Shows the blocked status, which is Blocked or Not Blocked.
If you include the optional *slot/port* information, the following additional information appears:	
Disable Reason	If the captive portal is disabled, this field indicates the reason.

Field	*Description*
Authenticated Users	Shows the number of authenticated users connected to the network through this captive portal.

show captive-portal configuration status

This command displays information of all configured captive portal configurations or a specific captive portal configuration.

Format **show captive-portal configuration** *<cp-id>* **status**

Mode Privileged EXEC

Field	*Description*
CP ID	Shows the captive portal ID.
CP Name	Shows the captive portal name.
CP Mode	Shows whether the CP is enabled or disabled.
Protocol Mode	Shows the current connection protocol, which is either HTTP or HTTPS.
Verification Mode	Shows the current account type, which is Guest, Local, or RADIUS.
If you include the optional `[cp-id]` **status** keywords, the following additional information appears:	
URL Redirect Mode	Indicates whether the Redirect URL Mode is enabled or disabled.
Max Bandwidth Up (bytes/sec)	The maximum rate in bytes per second (bps) at which a client can send data into the network.
Max Bandwidth Down (bytes/sec)	The maximum rate in bps at which a client can receive data from the network.
Max Input Octets (bytes)	The maximum number of octets the user is allowed to transmit.
Max Output Octets (bytes)	The maximum number of octets the user is allowed to receive.
Max Total Octets (bytes)	The maximum number of octets the user is allowed to transfer, i.e., the sum of octets transmitted and received.
Session Timeout (seconds)	Shows 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)	Shows 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.

show captive-portal configuration locales

This command displays locales associated with a specific captive portal configuration.

Format **show captive-portal configuration** *<cp-id>* **locales**

Mode Privileged EXEC

Field	*Description*
Locale Code	Two-letter abbreviation for languages.

Field	*Description*
Locale Link	The names of the languages.

CAPTIVE PORTAL CLIENT CONNECTION COMMANDS

Use the commands in this section to view information about the clients connected to the captive portals configured on the switch.

show captive-portal client status

This command displays client connection details or a connection summary for connected captive portal users. Use the optional *[macaddr]* keyword, which is the MAC address of a client, to view additional information about that client.

Format	**show captive-portal client** *[macaddr]* **status**
Mode	Privileged EXEC

Field	*Description*
Client MAC Address	Identifies the MAC address of the wireless client (if applicable).
Client IP Address	Identifies the IP address of the wireless client (if applicable).
Protocol Mode	Shows the current connection protocol, which is either HTTP or HTTPS.
Verification Mode	Shows the current account type, which is Guest, Local, or RADIUS.
Session Time	Shows the amount of time that has passed since the client was authorized.
If you specify a client MAC address, the following additional information displays:	
CP ID	Shows the captive portal ID the connected client is using.
CP Name	Shows the name of the captive portal the connected client is using.
Interface	Valid slot and port number separated by a forward slash.
Interface Description	Describes the interface.
User Name	Displays the user name (or Guest ID) of the connected client.
If cluster support is available, the following fields display:	
Switch MAC Address	Identifies the MAC address of the switch (if applicable).
Switch IP Address	Identifies the IP address of the switch (if applicable).
Switch Type (local or peer)	Shows the current switch type, which is local or peer.

show captive-portal client statistics

This command displays the statistics for a specific captive portal client.

Format	**show captive-portal client** *<macaddr>* **statistics**
Mode	Privileged EXEC

Field	*Description*
Client MAC Address	Identifies the MAC address of the wireless client (if applicable).
Bytes Received	Total bytes the client has received.
Bytes Transmitted	Total bytes the client has transmitted.
Packets Transmitted	Total packets the client has transmitted.
Packets Received	Total packets the client has received.

show captive-portal interface client status

This command displays information about clients authenticated on all interfaces or a specific interface.

Format **show captive-portal interface** *[slot/port]* **client status**

Mode Privileged EXEC

Field	*Description*
Interface	Valid slot and port number separated by a forward slash.
Interface Description	Describes the interface.
Client MAC Address	Identifies the MAC address of the wireless client (if applicable).
If you use the optional *[slot/port]* information, the following additional information appears:	
Client IP Address	Identifies the IP address of the wireless client (if applicable).
CP ID	Shows the captive portal ID the connected client is using.
CP Name	Shows the name of the captive portal the connected client is using.
Protocol	Shows the current connection protocol, which is either HTTP or HTTPS.
Verification	Shows the current account type, which is Guest, Local, or RADIUS.
User Name	Displays the user name (or Guest ID) of the connected client.

show captive-portal configuration client status

This command displays the clients authenticated to all captive portal configurations or a specific configuration.

Format **show captive-portal configuration** *[cp-id]* **client status**

Mode Privileged EXEC

Field	*Description*
CP ID	Shows the captive portal ID the connected client is using.
CP Name	Shows the name of the captive portal the connected client is using.
Client MAC Address	Identifies the MAC address of the wireless client (if applicable).
If you use the optional *[cp-id]* information, the following additional information appears:	

Field	*Description*
Client IP Address	Identifies the IP address of the wireless client (if applicable).
Interface	Valid slot and port number separated by a forward slash.
Interface Description	Describes the interface.

captive-portal client deauthenticate

This command deauthenticates a specific captive portal client. You can specify a captive portal configuration ID from 1-10 to indicate the captive portal configuration that the client is deauthenticating from. If no value is entered, then the specified clients (or all clients) are deauthenticated from all captive portal configurations.

You can use the *<macaddr>* variable to specify the MAC address of the client to deauthenticate. If no value is specified, then all clients are deauthenticated from the specified captive portal configuration (or all configurations).

Format **captive-portal client deauthenticate** *<1-10> <macaddr>*

Mode Privileged EXEC

CAPTIVE PORTAL INTERFACE COMMANDS

Use the commands in this section to view information about the interfaces on the switch that are associated with captive portals or that are capable of supporting a captive portal.

show captive-portal interface configuration status

This command displays the interface to configuration assignments for all captive portal configurations or a specific configuration.

Format **show captive-portal interface configuration** *[cp-id]* **status**

Mode Privileged EXEC

Field	*Description*
CP ID	Shows the captive portal ID the connected client is using.
CP Name	Shows the name of the captive portal the connected client is using.
Interface	Valid slot and port number separated by a forward slash.
Interface Description	Describes the interface.
Type	Shows the type of interface.

show captive-portal interface capability

This command displays all the captive portal eligible interfaces or the interface capabilities for a specific captive portal interface.

Format **show captive-portal interface capability** *[slot/port]*

Mode Privileged EXEC

Field	*Description*
Interface	Valid slot and port number separated by a forward slash.
Interface Description	Describes the interface.
Type	Shows the type of interface.
If you use the optional [*slot/port*] information, the following additional information appears:	
Session Timeout	Indicates whether or not this field is supported by the specified captive portal interface.
Idle Timeout	Indicates whether or not this field is supported by the specified captive portal interface.
Bytes Received Counter	Indicates whether or not this field is supported by the specified captive portal interface.
Bytes Transmitted Counter	Indicates whether or not this field is supported by the specified captive portal interface.
Packets Received Counter	Indicates whether or not this field is supported by the specified captive portal interface.

Field	*Description*
Packets Transmitted Counter	Indicates whether or not this field is supported by the specified captive portal interface.
Roaming	Indicates whether or not this field is supported by the specified captive portal interface.

CAPTIVE PORTAL LOCAL USER COMMANDS

Use these commands to view and configure captive portal users in the local database.

user (Captive Portal Config Mode)

This command is used to create a local user. The *<user-id>* variable is the user ID, which can be a number between 1 and 128. The password is 8-64 characters. You can modify the password after you create the user by using this command with the user ID and a new password.

There are two ways to create the user: using `name` and using `password`. If the user is created using `name`, the password needs to be assigned with the user password command. Or, if the user is created using password, the name can be assigned later:

Format **user** *<user-id>* **name** *<password>*
Mode Captive Portal Config

Format **user** *<user-id>* **password** *<password>*
Mode Captive Portal Config

Example: The following shows an example using `name` to create the user.

```
(DWS-4026)(Config-CP) #user 1 name test
```

Example: The following shows an example using `password` to create the user.

```
(DWS-4026)(Config-CP) #user 1 password test1234<cr>
```

no user

This command deletes a user from the local user database. If the user has an existing session, it is disconnected.

Format **no user** *<user-id>*
Mode Captive Portal Config

Example: The following shows an example of the command.

```
(DWS-4026)(Config-CP) #no user 1<cr>
```

user name

This command assigns a name to the User ID. This name is used at the client station for authentication. The *<user-id>* variable is the local user ID created with the **user** command and can be from 1 to 128 characters. The *<username>* variable is the name of the user and can have up to 32 alphanumeric characters.

Format **user** *<user-id>* **name** *<username>*
Mode Captive Portal Config

Example: The following shows an example of the command.

```
(DWS-4026)(Config-CP) #user 1 name johnsmith<cr>
```

user password

This command sets or modifies the password for the associated captive portal user. The *<user-id>* variable is the local user ID created with the **user** command and can be from 1 to 128 characters. The *<password>* variable is the user id's password and can have from 8 to 64 alphanumeric characters.

Format	**user** *<user-id>* **password** *<password>*
Mode	Captive Portal Config

Example: The following shows an example of the command.

```
(DWS-4026)(Config-CP) #user 1 password<cr>
Enter Password (8 - 64 characters):<enter here>
Re-enter password:<enter same here>
```

user password encrypted

This command modifies the password for the associated captive portal user. The command accepts the password in an encrypted format. This command is used primarily by the `show running config` command process.

The *<user-id>* variable is the local user ID created with the **user** command. The *<encrypt-pwd>* variable is the password in encrypted format, which can be up to 128 hexadecimal characters.

Format	**user** *<user-id>* **password encrypted** *<encrypted-pwd>*
Mode	Captive Portal Config

Example: The following shows an example of the command.

```
(DWS-4026)(Config-CP) #user 1 password encrypted <encrypted-pwd><cr>
```

user group

This command assigns/modifies the group name for the associated captive portal user. The *<user-id>* variable is the user ID, which is a number in the range of 1 to 128. The *<group-name>* variable is a name up to 32 characters.

Format	**user** *<user-id>* **group** *<group-name>*
Mode	Captive Portal Config

Example: The following shows an example of the command.

```
(DWS-4026)(Config-CP) #user 1 group 123<cr>
```

user session-timeout

This command sets the session timeout value for the associated captive portal user. The *<user-id>* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128. The *<timeout>* variable is a number that represents the session timeout in seconds. Use 0 to indicate that the timeout is not enforced.

Default	0
Format	**user** *<user-id>* **session-timeout** *<timeout>*
Mode	Captive Portal Config

Example: The following shows an example of the command.

```
(DWS-4026)(Config-CP) #user 1 session-timeout 86400<cr>
```

no user session-timeout

This command sets the session timeout value for the associated captive portal user to the default value. The *<user-id>* variable is a user configured in the local database.

Format	**no user** *<user-id>* **session-timeout**
Mode	Captive Portal Config

Example: The following shows an example of the command.

```
(DWS-4026)(Config-CP) #no user 1 session-timeout<cr>
```

user idle-timeout

This command sets the session idle timeout value for the associated captive portal user. The *<user-id>* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128. The *<timeout>* variable is a number that represents the idle timeout in seconds. Use 0 to indicate that the timeout is not enforced.

Default	0
Format	**user** *<user-id>* **idle-timeout** *<timeout>*
Mode	Captive Portal Config

Example: The following shows an example of the command.

```
(DWS-4026)(Config-CP) #user 1 idle-timeout 600<cr>
```

no user idle-timeout

This command sets the session idle timeout value for the associated captive portal user to the default value. The *<user-id>* variable is a user configured in the local database.

Format	**no user** *<user-id>* **idle-timeout**
Mode	Captive Portal Config

Example: The following shows an example of the command.

```
(DWS-4026)(Config-CP) #no user 1 idle-timeout<cr>
```

user max-bandwidth-up

This command is used to configure the bandwidth in bytes per second (bps) at which the client can send data into the network. 0 denotes using the default value configured for the captive portal.

Default 0

Format **user** *<user-id>* **max-bandwidth-up** *<bps>*

Mode Captive Portal Config

Parameter	*Description*
user-id	User ID from 1 to 128 characters.
bps	Client transmit rate in bytes per second (bps). 0 denotes unlimited bandwidth.

no user max-bandwidth-up

Use this command to set to the default the bandwidth at which the client can send data into the network.

Format **no user** *<user-id>* **max-bandwidth-up**

Mode Captive Portal Config

user max-bandwidth-down

This command is used configure the bandwidth in bytes per second (bps) at which the client can receive data from the network. 0 denotes using the default value configured for the captive portal.

Default 0

Format **user** *<user-id>* **max-bandwidth-down** *<bps>*

Mode Captive Portal Config

Parameter	*Description*
user-id	User ID from 1 to 128 characters.
bps	Client receive rate in bps. 0 denotes unlimited bandwidth.

no user max-bandwidth down

Use this command to set to the default value the bandwidth at which the client can receive data from the network.

Format **no user** *<user-name>* **max-bandwidth-down**

Mode Captive Portal Config

user max-input-octets

This command is used 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. 0 octets denote unlimited transmission.

Default 0

Format **user** *<user-id>* **max-input-octets** *<octets>*

Mode Captive Portal Config

Parameter	Description
user-id	User ID from 1 to 128 characters.
octets	Number of bytes.

no user max-input-octets

Use this command to set to the default the number of octets in bytes that the user is allowed to transmit.

Format **no user** *<user-id>* **max-input-octets**
Mode Captive Portal Config

user max-output-octets

This command is used 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. 0 octets denote unlimited transmission.

Default 0
Format **user** *<user-id>* **max-output-octets** *<octets>*
Mode Captive Portal Config

Parameter	Description
user-id	User ID from 1 to 128 characters.
octets	Number of bytes.

no user max-output-octets

Use this command to set to the default the number of octets in bytes that the user is allowed to receive.

Format **no user** *<user-id>* **max-output-octets**
Mode Captive Portal Config

user max-total-octets

This command is used 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 octets transmitted and received. After this limit has been reached, the user will be disconnected. 0 octets denote unlimited transmission.

Default 0
Format **user** *<user-id>* **max-total-octets** *<octets>*
Mode Captive Portal Config

Parameter	Description
user-id	User ID from 1 to 128 characters.

Parameter	*Description*
octets	Number of bytes.

no user max-total-octets

Use this command to set to the default the number of octets in bytes that the user is allowed to transmit and receive.

Format **no user** *<user-id>* **max-total-octets**

Mode Captive Portal Config

show captive-portal user

This command displays all configured users or a specific user in the captive portal local user database. Enter the optional user ID to view information about the specified user. The ***[user-id]*** variable is a valid user configured in the local database. Enter the **group** keyword or the **group** keyword and group ID variable to view the user information organized by groups.

Format **show captive-portal user** *[user-id] [group [<group-id>]]*

Mode Privileged EXEC

Field	*Description*
User ID	Displays the ID of the user.
User Name	Displays the user name.
Session Timeout	Displays the number of seconds the user can remain in a session before being disconnected from the Captive Portal.
Idle Timeout	Displays the number of seconds the user can remain idle before being disconnected from the Captive Portal.
Group ID	Displays the group identifier for the group to which the user belongs.
When you include the *[user-id]* variable, the following information also displays:	
Password Configured	Indicates whether a password has been configured for the user.
Max Bandwidth Up (bps)	The maximum rate in bytes per second (bps) at which a client can send data into the network.
Max Bandwidth Down (bps)	The maximum rate in bps at which a client can receive data from the network.
Max Bandwidth Input Octets (bytes)	The maximum number of octets the user is allowed to transmit.
Max Bandwidth Output Octets (bytes)	The maximum number of octets the user is allowed to receive.
Max Bandwidth Total Octets (bytes)	The maximum number of octets the user is allowed to transfer, i.e., the sum of octets transmitted and received.

clear captive-portal users

This command deletes all captive portal user entries.

Format	`clear captive-portal users`
Mode	Privileged EXEC

CAPTIVE PORTAL USER GROUP COMMANDS

Use the following commands to configure CP user groups.

user group

Use this command to create a user group. The *<group-id>* variable is a number in the range of 1-10.

Format	**user group** *<group-id>*
Mode	Captive Portal Config

no user group

Use this command to delete a user group.

Format	**no user group** *<group-id>*
Mode	Captive Portal Config

user group name

Use this command to configure a group name. The *<group-id>* variable is a number in the range of 1-10. The *<name>* variable can be up to 32 alphanumeric characters.

Format	**user group** *<group-id>* **name** *<name>*
Mode	Captive Portal Config

user group rename

This command replaces a group's associations with the default group or a specified group. The *<group-id>* and ***<new-group-id>*** variables are each a number in the range of 1-10.

Format	**user group** *<group-id>* **rename** *<new-group-id>*
Mode	Captive Portal Config

Section 7: Quality of Service Commands

This section describes the Quality of Service (QoS) commands available in the Unified Switch CLI.

The QoS Commands section contains the following subsections:

Note: The commands in this section are in one of two functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

Class of Service Commands

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.

Note: Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class. The *<userpriority>* values can range from 0-7. The *<trafficclass>* values range from 0-6, although the actual number of available traffic classes depends on the platform. For more information about 802.1p priority, see "Voice VLAN Commands" on page 45.

Format `classofservice dot1p-mapping` *<userpriority> <trafficclass>*

Modes
- Global Config
- Interface Config

no classofservice dot1p-mapping

This command maps each 802.1p priority to its default internal traffic class value.

Format **no classofservice dot1p-mapping**

Modes
- Global Config
- Interface Config

classofservice ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class. The *<ipdscp>* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

The *<trafficclass>* values can range from 0-6, although the actual number of available traffic classes depends on the platform.

Format **classofservice ip-dscp-mapping** *<ipdscp> <trafficclass>*

Mode Global Config

no classofservice ip-dscp-mapping

This command maps each IP DSCP value to its default internal traffic class value.

Format **no classofservice ip-dscp-mapping**

Mode Global Config

classofservice trust

This command sets the class of service trust mode of an interface. You can set the mode to trust one of the Dot1p (802.1p) or IP DSCP packet markings. You can also set the interface mode to untrusted. If you configure an interface to use Dot1p, the mode does not appear in the output of the **show running config** command because Dot1p is the default.

Note: The **classofservice trust dot1p** command will not be supported in future releases of the software because Dot1p is the default value. Use the **no classofservice trust** command to set the mode to the default value.

Default dot1p

Format **classofservice trust** *{dot1p | ip-dscp | untrusted}*

Modes
- Global Config
- Interface Config

no classofservice trust

This command sets the interface mode to the default value.

Format **no classofservice trust**

Modes
- Global Config
- Interface Config

cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue. The total number of queues supported per interface is 8. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

Format **cos-queue min-bandwidth** *<bw-0> <bw-1> … <bw-7>*

Modes
- Global Config
- Interface Config

no cos-queue min-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format **no cos-queue min-bandwidth**

Modes
- Global Config
- Interface Config

cos-queue strict

This command activates the strict priority scheduler mode for each specified queue.

Format **cos-queue strict** *<queue-id-0> [<queue-id-2> … <queue-id-7>]*

Modes
- Global Config
- Interface Config

no cos-queue strict

This command restores the default weighted scheduler mode for each specified queue.

Format **no cos-queue strict** *<queue-id-0> [<queue-id-2> … <queue-id-7>]*

Modes
- Global Config
- Interface Config

traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Format **traffic-shape** *<bw>*

Modes
- Global Config
- Interface Config

no traffic-shape

This command restores the interface shaping rate to the default value.

Format	**`no traffic-shape`**
Modes	• Global Config • Interface Config

show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. The *<slot/port>* parameter is optional. If specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed. For more information, see "Voice VLAN Commands" on page 45.

Format	**`show classofservice dot1p-mapping`** *[<slot/port>]*
Mode	Privileged EXEC

The following information is repeated for each user priority.

Term	Definition
User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show classofservice dot1p-mapping

 User Priority    Traffic Class
 -------------    -------------
       0                1
       1                0
       2                0
       3                1
       4                2
       5                2
       6                7
       7                3
```

The following information is repeated for each user priority.

Term	***Definition***
IP Precedence	The IP Precedence value.
Traffic Class	The traffic class internal queue identifier to which the IP Precedence value is mapped.

show classofservice ip-dscp-mapping

This command displays the current IP DSCP mapping to internal traffic classes for the global configuration settings.

Format **show classofservice ip-dscp-mapping**

Mode Privileged EXEC

The following information is repeated for each user priority.

Term	*Definition*
IP DSCP	The IP DSCP value.
Traffic Class	The traffic class internal queue identifier to which the IP DSCP value is mapped.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show classofservice ip-dscp-mapping

    IP DSCP       Traffic Class
 -------------    -------------
   0(be/cs0)           1
   1                   1
   2                   1
   3                   1
   4                   1
   5                   1
   6                   1
   7                   1
   8(cs1)              0
   9                   0
   10(af11)            0
   11                  0
   12(af12)            0
   13                  0
   14(af13)            0
   15                  0
   16(cs2)             0
   17                  0
   18(af21)            0
   19                  0
--More-- or (q)uit
```

show classofservice trust

This command displays the current trust mode setting for a specific interface. The *<slot/port>* parameter is optional. If you specify an interface, the command displays the port trust mode of the interface. If you do not specify an interface, the command displays the most recent global configuration settings.

Format **show classofservice trust** *[<slot/port>]*

Mode Privileged EXEC

Term	*Definition*
Non-IP Traffic Class	The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to trust IP Precedence or IP DSCP (on platforms that support IP DSCP).
Untrusted Traffic Class	The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show classofservice trust 0/1

Class of Service Trust Mode: Untrusted

Untrusted Traffic Class: 1
```

show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. The slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format **show interfaces cos-queue** *[<slot/port>]*

Mode Privileged EXEC

Term	*Definition*
Queue Id	An interface supports 8 queues numbered 0 to 7.
Minimum Bandwidth	The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.
Queue Management Type	The queue depth management technique used for this queue (tail drop).

If you specify the interface, the command also displays the following information.

Term	*Definition*
Interface	The slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.
Interface Shaping Rate	The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface. This is a configured value.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show interfaces cos-queue 0/1

Interface..................................... 0/1
Interface Shaping Rate........................ 64

Queue Id   Min. Bandwidth   Scheduler Type   Queue Management Type
```



```
--------   --------------   --------------   ---------------------
0          10               Weighted         Tail Drop
1          10               Weighted         Tail Drop
2          10               Weighted         Tail Drop
3          10               Weighted         Tail Drop
4          10               Weighted         Tail Drop
5          10               Weighted         Tail Drop
6          10               Weighted         Tail Drop
7          10               Weighted         Tail Drop
```

DIFFERENTIATED SERVICES COMMANDS

This section describes the commands you use to configure QOS Differentiated Services (DiffServ).

You configure DiffServ in several stages by specifying three DiffServ components:

1. Class
   a. Creating and deleting classes.
   b. Defining match criteria for a class.
2. Policy
   a. Creating and deleting policies
   b. Associating classes with a policy
   c. Defining policy statements for a policy/class combination
3. Service
   a. Adding and removing a policy to/from an inbound interface

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:

- Each class can contain a maximum of one referenced (nested) class
- Class definitions do not support hierarchical service policies

A given class definition can contain a maximum of one reference to another class. You can combine the reference with other match criteria. The referenced class is truly a reference and not a copy since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes, otherwise the switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

Note: The mark possibilities for policing include CoS, IP DSCP, and IP Precedence. While the latter two are only meaningful for IP packet types, CoS marking is allowed for both IP and non-IP packets, since it updates the 802.1p user priority field contained in the VLAN tag of the layer 2 packet header.

diffserv

This command sets the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format	**diffserv**
Mode	Global Config

no diffserv

This command sets the DiffServ operational mode to inactive. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format	**no diffserv**
Mode	Global Config

DIFFSERV CLASS COMMANDS

Use the DiffServ class commands to define traffic classification. To classify traffic, you specify Behavior Aggregate (BA), based on DSCP and Multi-Field (MF) classes of traffic (name, match criteria)

This set of commands consists of class creation/deletion and matching, with the class match commands specifying Layer 3, Layer 2, and general match criteria. The class match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic that belongs to the class.

Note: Once you create a class match criterion for a class, you cannot change or delete the criterion. To change or delete a class match criterion, you must delete and re-create the entire class.

The CLI command root is **class-map**.

class-map

This command defines a DiffServ class of type match-all. When used without any match condition, this command enters the class-map mode. The *<class-map-name>* is a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class.

Note: The class-map-name 'default' is reserved and must not be used.

The class type of **match-all** indicates all of the individual match conditions must be true for a packet to be considered a member of the class.This command may be used without specifying a class type to enter the Class-Map Config mode for an existing DiffServ class.

Note: The CLI mode is changed to Class-Map Config or when this command is successfully executed.

Format	**class-map match-all** *<class-map-name>*
Mode	Global Config

no class-map

This command eliminates an existing DiffServ class. The *<class-map-name>* is the name of an existing DiffServ class. (The class name **default** is reserved and is not allowed here.) This command may be issued at any time; if the class is currently referenced by one or more policies or by any other class, the delete action fails.

Format **no class-map** *<class-map-name>*

Mode Global Config

class-map rename

This command changes the name of a DiffServ class. The *<class-map-name>* is the name of an existing DiffServ class. The *<new-class-map-name>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

Default none

Format **class-map rename** *<class-map-name> <new-class-map-name>*

Mode Global Config

match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class.

Default none

Format **match any**

Mode Class-Map Config

match class-map

This command adds to the specified class definition the set of match conditions defined for another class. The *<refclassname>* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Default none

Format **match class-map** *<refclassname>*

Mode Class-Map Config

Note:

- The parameters *<refclassname>* and *<class-map-name>* can not be the same.
- Only one other class may be referenced by a class.
- Any attempt to delete the *<refclassname>* class while the class is still referenced by any *<class-map-name>* fails.
- The combined match criteria of *<class-map-name>* and *<refclassname>* must be an allowed combination based on the class type.
- Any subsequent changes to the *<refclassname>* class match criteria must maintain this validity, or the change attempt fails.
- The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed 12. In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.

no match class-map

This command removes from the specified class definition the set of match conditions defined for another class. The *<refclassname>* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Format	**no match class-map** *<refclassname>*
Mode	Class-Map Config

match dstip

This command adds to the specified class definition a match condition based on the destination IP address of a packet. The *<ipaddr>* parameter specifies an IP address. The *<ipmask>* parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits.

Default	none
Format	**match dstip** *<ipaddr> <ipmask>*
Mode	Class-Map Config

match dstl4port

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword, the value for *<portkey>* is one of the supported port name keywords. The currently supported *<portkey>* values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number. To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535.

Default	none
Format	**match dstl4port** *{<portkey> | <0-65535>}*
Mode	Class-Map Config Ipv6-Class-Map Config

match ip dscp

This command adds to the specified class definition a match condition based on 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).

The *<dscpval>* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Note: The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default	none
Format	**match ip dscp** *<dscpval>*
Mode	Class-Map Config Ipv6-Class-Map Config

match ip precedence

This command adds to the specified class definition a match condition based on the value of the IP Precedence field 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). The precedence value is an integer from 0 to 7.

Note: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default	none
Format	**match ip precedence** *<0-7>*
Mode	Class-Map Config

match ip tos

This command adds to the specified class definition a match condition based on the value of the IP TOS field in a packet, which is defined as all eight bits of the Service Type octet in the IP header. The value of *<tosbits>* is a two-digit hexadecimal number from 00 to ff. The value of *<tosmask>* is a two-digit hexadecimal number from 00 to ff. The *<tosmask>* denotes the bit positions in *<tosbits>* that are used for comparison against the IP TOS field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a *<tosbits>* value of a0 (hex) and a *<tosmask>* of a2 (hex).

Note: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Note: This “free form” version of the IP DSCP/Precedence/TOS match specification gives the user complete control when specifying which bits of the IP Service Type field are checked.

Default	none
Format	**match ip tos** *<tosbits> <tosmask>*
Mode	Class-Map Config

match protocol

This command adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

To specify the match condition using a single keyword notation, the value for <protocol-name> is one of the supported protocol name keywords. The currently supported values are: *icmp*, *igmp*, *ip*, *tcp*, *udp*. A value of *ip* matches all protocol number values.

To specify the match condition using a numeric value notation, the protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255.

Note: This command does not validate the protocol number value against the current list defined by IANA.

Default	none
Format	**match protocol** *{<protocol-name> | <0-255>}*
Mode	Class-Map Config Ipv6-Class-Map Config

match srcip

This command adds to the specified class definition a match condition based on the source IP address of a packet. The *<ipaddr>* parameter specifies an IP address. The *<ipmask>* parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits.

Default	none
Format	**match srcip** *<ipaddr> <ipmask>*
Mode	Class-Map Config

match srcip6

This command adds to the specified class definition a match condition based on the source IP address of a packet.

Default	none
Format	**match srci**p6 <source-ipv6-prefix/prefix-length>
Mode	Ipv6-Class-Map Config

match srcl4port

This command adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword notation, the value for *<portkey>* is one of the supported port name keywords (listed below). The currently supported *<portkey>* values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one layer 4 port number is required. The port number is an integer from 0 to 65535.

Default	none
Format	**match srcl4port** *{<portkey> | <0-65535>}*
Mode	Class-Map Config Ipv6-Class-Map Config

DIFFSERV POLICY COMMANDS

Use the DiffServ policy commands to specify traffic conditioning actions, such as policing and marking, to apply to traffic classes

Use the policy commands to associate a traffic class that you define by using the class command set with one or more QoS policy attributes. Assign the class/policy association to an interface to form a service. Specify the policy name when you create the policy.

Each traffic class defines a particular treatment for packets that match the class definition. You can associate multiple traffic classes with a single policy. When a packet satisfies the conditions of more than one class, preference is based on the order in which you add the classes to the policy. The first class you add has the highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes.

Note: The only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

The CLI command root is **policy-map**.

assign-queue

This command modifies the queue id to which the associated traffic stream is assigned. The *queueid* is an integer from 0 to 7 and the number of egress queues supported by the switch is 8.

Format	**assign-queue** *<queueid>*
Mode	Policy-Class-Map Config
Incompatibilities	Drop

drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format	**drop**
Mode	Policy-Class-Map Config
Incompatibilities	Assign Queue, Mark (all forms), Mirror, Police

mirror

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

Format	**mirror** *<slot/port>*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Redirect

conform-color

Use this command to enable color-aware traffic policing and define the conform-color class map. Used in conjunction with the police command where the fields for the conform level are specified. The <class-map-name> parameter is the name of an existing DiffServ class map.

Note: This command may only be used after specifying a police command for the policy-class instance.

Format	**conform-color** *<class-map-name>*
Mode	Policy-Class-Map Config

class

This command creates 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. The *<classname>* is the name of an existing DiffServ class.

Note: This command causes the specified policy to create a reference to the class definition.

Note: The CLI mode is changed to Policy-Class-Map Config when this command is successfully executed.

Format	**class** *<classname>*
Mode	Policy-Map Config

no class

This command deletes the instance of a particular class and its defined treatment from the specified policy. *<classname>* is the names of an existing DiffServ class.

Note: This command removes the reference to the class definition for the specified policy.

Format	**no class** *<classname>*
Mode	Policy-Map Config

mark cos

This command marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

Default	1
Format	**mark-cos** *<0-7>*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

mark ip-dscp

This command marks all packets for the associated traffic stream with the specified IP DSCP value.

The *<dscpval>* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef .

Format	**mark ip-dscp** *<dscpval>*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police

mark ip-precedence

This command marks all packets for the associated traffic stream with the specified IP Precedence value. The IP Precedence value is an integer from 0 to 7.

Format	**mark ip-precedence** *<0-7>*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police

police-simple

This command is used to establish the traffic policing style for the specified class. The simple form of the police command uses a single data rate and burst size, resulting in two outcomes: conform and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

For each outcome, the only possible actions are drop, set-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop.

For set-dscp-transmit, a *<dscpval>* value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.

For set-cos-transmit an 802.1p priority value is required and is specified as an integer from 0-7.

Format	**police-simple** *{<1-4294967295> <1-128> conform-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | transmit} [violate-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | transmit}]}*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark (all forms)

policy-map

This command establishes a new DiffServ policy. The *<policyname>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to the inbound traffic direction as indicated by the in parameter.

Note: The CLI mode is changed to Policy-Map Config when this command is successfully executed.

Format	**policy-map** *<policyname>* **in**
Mode	Global Config

no policy-map

This command eliminates an existing DiffServ policy. The *<policyname>* parameter is the name of an existing DiffServ policy. This command may be issued at any time. If the policy is currently referenced by one or more interface service attachments, this delete attempt fails.

Format	**no policy-map** *<policyname>*
Mode	Global Config

policy-map rename

This command changes the name of a DiffServ policy. The *<policyname> i*s the name of an existing DiffServ class. The *<newpolicyname>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

Format	**policy-map rename** *<policyname> <newpolicyname>*
Mode	Global Config

DIFFSERV SERVICE COMMANDS

Use the DiffServ service commands to assign a DiffServ traffic conditioning policy, which you specified by using the policy commands, to an interface in the incoming direction

The service commands attach a defined policy to a directional interface. You can assign only one policy at any one time to an interface in the inbound direction. DiffServ is not used in the outbound direction.

This set of commands consists of service addition/removal.

The CLI command root is **service-policy**.

service-policy

This command attaches a policy to an interface in the inbound direction. The *<policyname>* parameter is the name of an existing DiffServ policy. This command causes a service to create a reference to the policy.

Note: This command effectively enables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.

Note: This command fails if any attributes within the policy definition exceed the capabilities of the interface. Once a policy is successfully attached to an interface, any attempt to change the policy definition, that would result in a violation of the interface capabilities, causes the policy change attempt to fail.

Format **service-policy in** *<policymapname>*

Modes
- Global Config
- Interface Config

Note: Each interface can have one policy attached.

no service-policy

This command detaches a policy from an interface in the inbound direction. The *<policyname>* parameter is the name of an existing DiffServ policy.

Note: This command causes a service to remove its reference to the policy. This command effectively disables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.

Format **no service-policy in** *<policymapname>*

Modes
- Global Config
- Interface Config

DIFFSERV SHOW COMMANDS

Use the DiffServ show commands to display configuration and status information for classes, policies, and services. You can display DiffServ information in summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled.

show class-map

This command displays all configuration information for the specified class. The *<class-name>* is the name of an existing DiffServ class.

Format **show class-map** *<class-name>*

Modes
- Privileged EXEC
- User EXEC

If the class-name is specified the following fields are displayed:

Term	*Definition*
Class Name	The name of this class.
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
L3 Proto	The Layer 3 protocol for this class. The Unified Switch currently only supports IPv4.
Match Criteria	The Match Criteria fields are only displayed if they have been configured. Not all platforms support all match criteria values. They are displayed in the order entered by the user. The fields are evaluated in accordance with the class type. The possible Match Criteria fields are: Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Ethertype, Source MAC Address, VLAN, Class of Service, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, and Source Layer 4 Port.
Values	The values of the Match Criteria.

If you do not specify the Class Name, this command displays a list of all defined DiffServ classes. The following fields are displayed:

Term	*Definition*
Class Name	The name of this class. (Note that the order in which classes are displayed is not necessarily the same order in which they were created.)
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Ref Class Name	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show class-map test

Class Name..................................... test
Class Type..................................... All
Class Layer3 Protocol.......................... ipv4

      Match Criteria                           Values
-------------------------- ------------------------------------------
Protocol                   99
```


show diffserv

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables. This command takes no options.

Format `show diffserv`

Mode Privileged EXEC

Term	*Definition*
DiffServ Admin mode	The current value of the DiffServ administrative mode.
Class Table Size	The current number of entries (rows) in the Class Table.
Class Table Max	The maximum allowed entries (rows) for the Class Table.
Class Rule Table Size	The current number of entries (rows) in the Class Rule Table.
Class Rule Table Max	The maximum allowed entries (rows) for the Class Rule Table.
Policy Table Size	The current number of entries (rows) in the Policy Table.
Policy Table Max	The maximum allowed entries (rows) for the Policy Table.
Policy Instance Table Size	Current number of entries (rows) in the Policy Instance Table.
Policy Instance Table Max	Maximum allowed entries (rows) for the Policy Instance Table.
Policy Attribute Table Size	Current number of entries (rows) in the Policy Attribute Table.
Policy Attribute Table Max	Maximum allowed entries (rows) for the Policy Attribute Table.
Service Table Size	The current number of entries (rows) in the Service Table.
Service Table Max	The maximum allowed entries (rows) for the Service Table.

show policy-map

This command displays all configuration information for the specified policy. The *<policyname>* is the name of an existing DiffServ policy.

Format `show policy-map` *[policyname]*

Mode Privileged EXEC

If the Policy Name is specified the following fields are displayed:

Term	*Definition*
Policy Name	The name of this policy.
Type	The policy type (Only inbound policy definitions are supported for this platform.)

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed):

Term	*Definition*
Assign Queue	Directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.
Class Name	The name of this class.

Term	*Definition*
Committed Burst Size (KB)	The committed burst size, used in simple policing.
Committed Rate (Kbps)	The committed rate, used in simple policing.
Conform Action	The current setting for the action taken on a packet considered to conform to the policing parameters. This is not displayed if policing is not in use for the class under this policy.
Conform COS	The CoS mark value if the conform action is set-cos-transmit.
Conform DSCP Value	The DSCP mark value if the conform action is set-dscp-transmit.
Conform IP Precedence Value	The IP Precedence mark value if the conform action is set-prec-transmit.
Drop	Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.
Mark CoS	The class of service value that is set in the 802.1p header of inbound packets. This is not displayed if the mark cos was not specified.
Mark IP DSCP	The mark/re-mark value used as the DSCP for traffic matching this class. This is not displayed if mark ip description is not specified.
Mark IP Precedence	The mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if mark ip precedence is not specified.
Non-Conform Action	The current setting for the action taken on a packet considered to not conform to the policing parameters. This is not displayed if policing not in use for the class under this policy.
Non-Conform COS	The CoS mark value if the non-conform action is set-cos-transmit.
Non-Conform DSCP Value	The DSCP mark value if the non-conform action is set-dscp-transmit.
Non-Conform IP Precedence Value	The IP Precedence mark value if the non-conform action is set-prec-transmit.
Policing Style	The style of policing, if any, used (simple).

If the Policy Name is not specified this command displays a list of all defined DiffServ policies. The following fields are displayed:

Term	Definition
Policy Name	The name of this policy. (The order in which the policies are displayed is not necessarily the same order in which they were created.)
Policy Type	The policy type (Only inbound is supported).
Class Members	List of all class names associated with this policy.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show policy-map p1

Policy Name..................................... p1
Policy Type..................................... In

Class Name...................................... test
This traffic will be dropped.
```


show diffserv service

This command displays policy service information for the specified interface and direction. The *<slot/port>* parameter specifies a valid slot/port number for the system.

Format **show diffserv service** *<slot/port>* **in**

Mode Privileged EXEC

Term	*Definition*
DiffServ Admin Mode	The current setting of the DiffServ administrative mode. An attached policy is only in effect on an interface while DiffServ is in an enabled mode.
Interface	Valid slot and port number separated by a forward slash.
Direction	The traffic direction of this interface service.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.
Policy Details	Attached policy details, whose content is identical to that described for the show policy-map *<policymapname>* command (content not repeated here for brevity).

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show diffserv service 0/1 in

DiffServ Admin Mode.......................... Enable
Interface.................................... 0/1
Direction.................................... In
No policy is attached to this interface in this direction.
```

show diffserv service brief

This command displays all interfaces in the system to which a DiffServ policy has been attached. The inbound direction parameter is optional.

Format **show diffserv service brief** *[in]*

Mode Privileged EXEC

Term	*Definition*
DiffServ Mode	The current setting of the DiffServ administrative mode. An attached policy is only active on an interface while DiffServ is in an enabled mode.

The following information is repeated for interface and direction (only those interfaces configured with an attached policy are shown):

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
Direction	The traffic direction of this interface service.
OperStatus	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show diffserv service brief in

DiffServ Admin Mode.............................. Enable

 Interface   Direction  OperStatus         Policy Name
----------- ----------- ---------- ------------------------------
3/1         In          Down        p1
```

show policy-map interface

This command displays policy-oriented statistics information for the specified interface and direction. The *<slot/port>* parameter specifies a valid interface for the system.

Note: This command is only allowed while the DiffServ administrative mode is enabled.

Format **show policy-map interface** *<slot/port> [in]*

Mode Privileged EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
Direction	The traffic direction of this interface service.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

The following information is repeated for each class instance within this policy:

Term	*Definition*
Class Name	The name of this class instance.
In Discarded Packets	A count of the packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show policy-map interface 0/1 in

Interface....................................... 0/1

Direction....................................... In
No in-bound policy is attached to this interface.
```

show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction.

Format **show service-policy in**

Mode Privileged EXEC

The following information is repeated for each interface and direction (only those interfaces configured with an attached policy are shown):

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface.

MAC ACCESS CONTROL LIST COMMANDS

This section describes the commands you use to configure MAC Access Control List (ACL) settings. MAC ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The maximum number of ACLs you can create is 100. The limit applies to all ACLs, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is 12.
- If you configure an IP ACL on an interface, you cannot configure a MAC ACL on the same interface.

mac access-list extended

This command creates a MAC Access Control List (ACL) identified by *<name>*, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. The *<name>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

Note: The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.

Format **mac access-list extended** *<name>*
Mode Global Config

no mac access-list extended

This command deletes a MAC ACL identified by *<name>* from the system.

Format **no mac access-list extended** *<name>*
Mode Global Config

mac access-list extended rename

This command changes the name of a MAC Access Control List (ACL). The *<name>* parameter is the name of an existing MAC ACL. The *<newname>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name *<newname>* already exists.

Format	**mac access-list extended rename** *<name> <newname>*
Mode	Global Config

{deny | permit} (MAC ACL)

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list.

Note: The 'no' form of this command is not supported, since the rules within a MAC ACL cannot be deleted individually. Rather, the entire MAC ACL must be deleted and re-specified.

Note: An implicit 'deny all' MAC rule always terminates the access list.

Note: The assign-queue and mirror attributes are configurable for a deny rule, but they have no operational effect.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported *<ethertypekey>* values are: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

Table 9: Ethertype Keyword and 4-digit Hexadecimal Value

Ethertype Keyword	*Corresponding Value*
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864
rarp	0x8035

The vlan and cos parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed <queue-id> value is 0–7, and the number of user-configurable queues available for the switch is 8. The *assign-queue* parameter is valid only for a **permit** rule.

The *mirror* parameter allows the traffic matching this rule to be copied to the specified *<slot/port>.*

Note: The special command form **{deny | permit} any any** is used to match all Ethernet layer 2 packets, and is the equivalent of the IP access list "match every" rule.

Format *{deny|permit} {<srcmac> | any} {<dstmac> | any} [<ethertypekey> | <0x0600-0xFFFF>] [vlan {eq <0-4095>}] [cos <0-7>] [[log] [assign-queue <queue-id>]] [{mirror | redirect} <slot/port>]*

Mode Mac-Access-List Config

mac access-group

This command either attaches a specific MAC Access Control List (ACL) identified by *<name>* to an interface, or associates it with a VLAN ID, in a given direction. The *<name>* parameter must be the name of an existing MAC ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other mac access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified mac access list replaces the currently attached mac access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The VLAN keyword is only valid in the 'Global Config' mode. The 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration.

Format **mac access-group** *<name> [vlan <vlan-id>]* **in** *[sequence <1-4294967295>]*

Modes
- Global Config
- Interface Config

no mac access-group

This command removes a MAC ACL identified by *<name>* from the interface in a given direction.

Format **no mac access-group** *<name> [vlan <vlan-id>]* **in**

Modes
- Global Config
- Interface Config

show mac access-lists

This command displays a MAC access list and all of the rules that are defined for the MAC ACL. Use the *[name]* parameter to identify a specific MAC ACL to display.

Format **show mac access-lists** *[name]*

Mode Privileged EXEC

Term	*Definition*
Rule Number	The ordered rule number identifier defined within the MAC ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Source MAC Address	The source MAC address for this rule.
Destination MAC Address	The destination MAC address for this rule.
Ethertype	The Ethertype keyword or custom value for this rule.
VLAN ID	The VLAN identifier value or range for this rule.
COS	The COS (802.1p) value for this rule.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The slot/port to which packets matching this rule are copied.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show mac access-lists m1

ACL Name: m1
Inbound Interface(s): 0/8

Rule Number: 1
Action..................................... deny
Match All.................................. TRUE
Mirror Interface........................... 0/2
```

IP ACCESS CONTROL LIST COMMANDS

This section describes the commands you use to configure IP Access Control List (ACL) settings. IP ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IP ACLs:

- Unified Switch software does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is 100. The limit applies to all ACLs, regardless of type.
- The maximum number of rules per IP ACL is 12.
- If you configure a MAC ACL on an interface, you cannot configure an IP ACL on the same interface.
- Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A **1** in a bit position of the ACL mask indicates the corresponding bit can be ignored.

access-list

This command creates an IP Access Control List (ACL) that is identified by the access list number, which is 1-99 for standard ACLs or 100-199 for extended ACLs. Table 10 describes the parameters for the **`access-list`** command.

IP Standard ACL:

Format **access-list** *<1-99> {deny | permit} {every | <srcip> <srcmask>} [log] [assign-queue <queue-id>] [mirror <slot/port>]*

Mode Global Config

IP Extended ACL:

Format **access-list** *<100-199> {deny | permit} {every | {{icmp | igmp | ip | tcp | udp | <number>} <srcip> <srcmask>[{eq {<portkey> | <0-65535>} <dstip> <dstmask> [{eq {<portkey>| <0-65535>}] [precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>] [log] [assign-queue <queue-id>] [mirror <slot/port>]*

Mode Global Config

Table 10: ACL Command Parameters

Parameter	*Description*
<1-99> or <100-199>	Range 1 to 99 is the access list number for an IP standard ACL. Range 100 to 199 is the access list number for an IP extended ACL.
{deny | permit}	Specifies whether the IP ACL rule permits or denies an action. ***Note:*** Assign-queue and mirror attributes are configurable for a deny rule, but they have no operational effect.
every	Match every packet.
{icmp | igmp | ip | tcp | udp | <number>}	Specifies the protocol to filter for an extended IP ACL rule.
<srcip> <srcmask>	Specifies a source IP address and source netmask for match condition of the IP ACL rule.
[{eq {<portkey> | <0-65535>}]	Specifies the source layer 4 port match condition for the IP ACL rule. You can use the port number, which ranges from 0-65535, or you specify the *<portkey>*, which can be one of the following keywords: *domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp*, and *www*. Each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range.
<dstip> <dstmask>	Specifies a destination IP address and netmask for match condition of the IP ACL rule.
[precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>]	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *dscp*, *precedence*, *tos/tosmask*.
[log]	Specifies that this rule is to be logged.
[assign-queue <queue-id>]	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
[mirror <slot/port>]	Specifies the mirror interface which is the slot/port to which packets matching this rule are copied.

no access-list

This command deletes an IP ACL that is identified by the parameter *<accesslistnumber>* from the system. The range for *<accesslistnumber>* 1-99 for standard access lists and 100-199 for extended access lists.

Format **no access-list** *<accesslistnumber>*

Mode Global Config

ip access-list

This command creates an extended IP Access Control List (ACL) identified by <*name*>, consisting of classification fields defined for the IP header of an IPv4 frame. The <*name*> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

Note: The CLI mode changes to IPv4-Access-List Config mode when you successfully execute this command.

Format	**ip access-list** *<name>*
Mode	Global Config

no ip access-list

This command deletes the IP ACL identified by <name> from the system.

Format	**no ip access-list** *<name>*
Mode	Global Config

ip access-list rename

This command changes the name of an IP Access Control List (ACL). The <*name*> parameter is the names of an existing IP ACL. The <new*name*> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

This command fails is an IP ACL by the name <new*name*> already exists.

Format	**ip access-list rename** *<name> <newname>*
Mode	Global Config

{deny | permit} (IP ACL)

This command creates a new rule for the current IP access list. Each rule is appended to the list of configured rules for the list.

Note: The 'no' form of this command is not supported, since the rules within an IP ACL cannot be deleted individually. Rather, the entire IP ACL must be deleted and re-specified.

Note: An implicit 'deny all' IP rule always terminates the access list.

Note: The *mirror* parameter allows the traffic matching this rule to be copied to the specified *<slot/port>*. The *assign-queue* parameter is only valid for a **permit** rule.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the every keyword or the protocol, source address, and destination address values must be specified. The source and destination IP address

fields may be specified using the keyword `any` to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed `<queue-id>` value is 0–7, and the number of user-configurable queues available for the switch is 8. The *`assign-queue`* parameter is valid only for a **`permit`** rule.

Format `{deny | permit} {every | {{icmp | igmp | ip | tcp | udp | <number>} <srcip> <srcmask> [{eq {<portkey> | <0-65535>} <dstip> <dstmask> [{eq {<portkey>| <0-65535>}] [precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>] [log] [assign-queue <queue-id>] [mirror <slot/port>]`

Mode Ipv4-Access-List Config

ip access-group

This command either attaches a specific IP ACL identified by `<accesslistnumber>` to an interface or associates with a VLAN ID in a given direction. The parameter `<name>` is the name of the Access Control List.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

Default none

Format **`ip access-group`** *`<accesslistnumber> <name> [vlan <vlan-id>]`* **`in>`***`[sequence <1-4294967295>]`*

Modes
- Interface Config
- Global Config

no ip access-group

This command removes a specified IP ACL from an interface.

Default none

Format **`no ip access-group`** *`<accesslistnumber> [vlan <vlan-id>]`* **`in`**

Mode
- Interface Config
- Global Config

acl-trapflags

This command enables the ACL trap mode.

Default disabled

Format **`acl-trapflags`**

Mode Global Config

no acl-trapflags

This command disables the ACL trap mode.

Format	**no acl-trapflags**
Mode	Global Config

show ip access-lists

This command displays an IP ACL *<accesslistnumber>* is the number used to identify the IP ACL.

Format	**show ip access-lists** *<accesslistnumber>*
Mode	Privileged EXEC

Note: Only the access list fields that you configure are displayed.

Term	*Definition*
Rule Number	The number identifier for each rule that is defined for the IP ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
Source IP Address	The source IP address for this rule.
Source IP Mask	The source IP Mask for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination IP Mask	The destination IP Mask for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
IP Precedence	The value specified IP Precedence.
IP TOS	The value specified for IP TOS.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The slot/port to which packets matching this rule are copied.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show ip access-lists 2

ACL ID: 2

Rule Number: 1
Action..................................... permit
```



```
Match All..................................... TRUE
Mirror Interface.............................. 0/3
```

show access-lists

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction.

Format **show access-lists interface** *<slot/port>* **in**

Mode Privileged EXEC

Term	*Definition*
ACL Type	Type of access list (IP, IPv6, or MAC).
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).

Example: The following shows example CLI display output for the command.

```
(DWS-4026) TBD
```

AUTO-VOICE OVER IP COMMANDS

This section describes the commands you use to configure Auto-Voice over IP (VoIP) commands. The Auto-VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class-of-service than ordinary traffic. When you enable the Auto-VoIP feature on an interface, the interface scans incoming traffic for the following call-control protocols:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

When a call-control protocol is detected, the switch assigns the traffic in that session to the highest CoS queue, which is generally used for time-sensitive traffic.

auto-voip all

Use this command to enable VoIP Profile on the interfaces of the switch.

Default	disabled
Format	`auto-voip all`
Mode	Global Config

no auto-voip all

Use this command to disable VoIP Profile on the interfaces of the switch.

Format	`no auto-voip all`
Mode	Global Config

auto-voip

Use this command to enable VoIP Profile on the interface.

Default	disabled
Format	`auto-voip`
Mode	Interface Config

no auto-voip

Use this command to disable VoIP Profile on the interface.

Format	`no auto-voip all`
Mode	Interface Config

show auto-voip

Use this command to display the VoIP Profile settings on the interface or interfaces of the switch.

Format `show auto-voip interface {<slot/port>|all}`

Mode Privileged EXEC

Field	*Description*
AutoVoIP Mode	The Auto VoIP mode on the interface.
Traffic Class	The CoS Queue or Traffic Class to which all VoIP traffic is mapped to. This is not configurable and defaults to the highest CoS queue available in the system for data traffic.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show auto-voip interface 0/1

Interface  Auto VoIP Mode Traffic Class
---------  -------------- -------------
0/1        Enabled        7
```


Section 8: Utility Commands

This section describes the utility commands available in the Unified Switch CLI.

The Utility Commands section includes the following subsections:

Note: The commands in this section are in one of four functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Copy commands transfer or save configuration and informational files to and from the switch.
- Clear commands clear some or all of the settings to factory defaults.

Dual Image Commands

Unified Switch software supports a dual image feature that allows the switch to have two software images in the permanent storage. You can specify which image is the active image to be loaded in subsequent reboots. This feature allows reduced down-time when you upgrade or downgrade the software.

delete

This command deletes the supplied image file from the permanent storage. The image to be deleted must be a backup image. If this image is the active image, or if this image is activated, an error message displays.

Format `delete {image1 | image2}`

Mode Privileged EXEC

boot system

This command activates the specified image. It will be the active-image for subsequent reboots and will be loaded by the boot loader. The current active-image is marked as the backup-image for subsequent reboots.

Format	**boot system** *<image-file-name>*
Mode	Privileged EXEC

show bootvar

This command displays the version information and the activation status for the current active and backup images

Format	**show bootvar**
Mode	Privileged EXEC

filedescr

This command associates a given text description with an image. Any existing description will be replaced.

Format	**filedescr** *{image1 | image2} <text-description>*
Mode	Privileged EXEC

update bootcode

This command updates the bootcode (boot loader) on the switch. The bootcode is read from the active-image for subsequent reboots.

Format	**update bootcode**
Mode	Privileged EXEC

SYSTEM INFORMATION AND STATISTICS COMMANDS

This section describes the commands you use to view information about system features, components, and configurations.

show arp switch

This command displays the contents of the IP stack's Address Resolution Protocol (ARP) table. The IP stack only learns ARP entries associated with the management interfaces (the network ports). ARP entries associated with routing interfaces are not listed.

Format	**show arp switch**
Mode	Privileged EXEC

Term	*Definition*
IP Address	IP address of the management interface or another device on the management network.
MAC Address	Hardware MAC address of that device.

Term	*Definition*
Interface	For a service port the output is *Management*. For a network port, the output is the slot/port of the physical interface.

show eventlog

This command displays the event log, which contains error messages from the system. The event log is not cleared on a system reset.

Format `show eventlog`

Mode Privileged EXEC

Term	*Definition*
File	The file in which the event originated.
Line	The line number of the event.
Task Id	The task ID of the event.
Code	The event code.
Time	The time this event occurred.
Unit	The unit for the event.

Note: Event log information is retained across a switch reset.

show hardware

This command displays inventory information for the switch.

Note: The **`show version`** command and the **`show hardware`** command display the same information. In future releases of the software, the **`show hardware`** command will not be available. For a description of the command output, see the command "show version" on page 411.

Format `show hardware`

Mode Privileged EXEC

show version

This command displays inventory information for the switch.

Note: The **`show version`** command will replace the **`show hardware`** command in future releases of the software.

Format `show version`

Mode Privileged EXEC

Term	*Definition*
Switch Description	Text used to identify the product name of this switch.
Machine Model	The machine model as defined by the Vital Product Data
Serial Number	The unique box serial number for this switch.
Burned in MAC Address	Universally assigned network address.
Software Version	The release.version.revision number of the code currently running on the switch.
Additional Packages	The additional packages incorporated into this system.

show interface

This command displays a summary of statistics for a specific interface or a count of all CPU traffic based upon the argument.

Format **show interface** *{<slot/port> | switchport}*

Mode Privileged EXEC

The display parameters, when the argument is *<slot/port>*, are as follows:

Parameters	*Definition*
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters, when the argument is “switchport” are as follows:

Term	*Definition*
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.

Term	*Definition*
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Address Entries Currently In Use	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
VLAN Entries Currently In Use	The number of VLAN entries presently occupying the VLAN table.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

show interface ethernet

This command displays detailed statistics for a specific interface or for all CPU traffic based upon the argument.

Format **`show interface ethernet`** *{<slot/port> | switchport}*

Mode Privileged EXEC

When you specify a value for *<slot/port>*, the command displays the following information.

Term	*Definition*
Media Type	The type of physical medium for the Ethernet. The possible values are 10Base-T, 100Base-TX, 100Base-FX, 1000Base-X, 1000Base-T and 10GBase-X.
ARP Type	Encapsulation type for the network address. The value is always ARPA.

Term	*Definition*
Packets Received	• **Total Packets Received (Octets)** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent. • **Packets Received 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets Received 65–127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 128–255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 256–511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 512–1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 1024–1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received > 1522 Octets** - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Packets RX and TX 64 Octets** - The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets RX and TX 65–127 Octets** - The total number of packets (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 128–255 Octets** - The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 256–511 Octets** - The total number of packets (including bad packets) received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 512–1023 Octets** - The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 1024–1518 Octets** - The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 1519–1522 Octets** - The total number of packets (including bad packets) received and transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 1523–2047 Octets** - The total number of packets received and transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Packets RX and TX 2048–4095 Octets** - The total number of packets received that were between 2048 and 4095 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Packets RX and TX 4096–9216 Octets** - The total number of packets received that were between 4096 and 9216 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.

Term	*Definition*
Packets Received Successfully	• **Total Packets Received Without Error** - The total number of packets received that were without errors. • **Unicast Packets Received** - The number of subnetwork-unicast packets delivered to a higher-layer protocol. • **Multicast Packets Received** - The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address. • **Broadcast Packets Received** - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received with MAC Errors	• **Total** - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. • **Jabbers Received** - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. • **Fragments/Undersize Received** - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets). • **Alignment Errors** - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets. • **Rx FCS Errors -** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. • **Overruns** - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Total Ignored Frames	The total number of dropped packets including those that were aborted.
Total Deferred Frames	The total number of frames that could not be transmitted after multiple attempts because they encountered collisions.
Packets Received with MAC Errors	• **Total** - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. • **Jabbers Received** - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. • **Fragments/Undersize Received** - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets). • **Alignment Errors** - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets. • **Rx FCS Errors -** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. • **Overruns** - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.

Term	*Definition*
Packets Transmitted Octets	• **Total Bytes** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. ----- • **Packets Transmitted 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets Transmitted 65-127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 128-255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 256-511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 512-1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 1024-1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Max Frame Size** - The maximum size of the Info (non-MAC) field that this port will receive or transmit.
Packets Transmitted Successfully	• **Total** - The number of frames that have been transmitted by this port to its segment. • **Unicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent. • **Multicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent. • **Broadcast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Errors	• **Total Errors** - The sum of Single, Multiple, and Excessive Collisions. • **Tx FCS Errors** - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. • **Oversized** - The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s. • **Underrun Errors** - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

Term	*Definition*
Transmit Discards	• **Total Discards** - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded. • **Total Output Packets Dropped** - The total number of Aged packets. • **Single Collision Frames** - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. • **Multiple Collision Frames** - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. • **Excessive Collision Frames** - A count of frames for which transmission on a particular interface fails due to excessive collisions. • **Late Collision Frames** - The total number of collisions that occur after 512 bit collision window has passed • **Port Membership Discards** - The number of frames discarded on egress for this port due to egress filtering being enabled. • **Lost/No Carrier Frames** - Loss of the carrier detection occurs when the carrier signal of the hardware is undetectable. It could be because the carrier signal was not present or was present but could not be detected. Each such event causes this counter to increase.
Protocol Statistics	• **802.3x Pause Frames Transmitted** - A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. • **GVRP PDUs Received** - The count of GVRP PDUs received in the GARP layer. • **GVRP PDUs Transmitted** - The count of GVRP PDUs transmitted from the GARP layer. • **GVRP Failed Registrations** - The number of times attempted GVRP registrations could not be completed. • **GMRP PDUs Received** - The count of GMRP PDU's received in the GARP layer. • **GMRP PDUs Transmitted** - The count of GMRP PDU's transmitted from the GARP layer. • **GMRP Failed Registrations** - The number of times attempted GMRP registrations could not be completed. • **STP BPDUs Transmitted** - Spanning Tree Protocol Bridge Protocol Data Units sent. • **STP BPDUs Received** - Spanning Tree Protocol Bridge Protocol Data Units received. • **RST BPDUs Transmitted** - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent. • **RSTP BPDUs Received** - Rapid Spanning Tree Protocol Bridge Protocol Data Units received. • **MSTP BPDUs Transmitted** - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent. • **MSTP BPDUs Received** - Multiple Spanning Tree Protocol Bridge Protocol Data Units received.
Dot1x Statistics	• **EAPOL Frames Received** - The number of valid EAPOL frames of any type that have been received by this authenticator. • **EAPOL Frames Transmitted** - The number of EAPOL frames of any type that have been transmitted by this authenticator.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

If you use the *switchport* keyword, the following information appears.

Term	*Definition*
Octets Received	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Total Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.

Term	*Definition*
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
Address Entries in Use	The number of Learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	The maximum number of Virtual LANs (VLANs) allowed on this switch.
Most VLAN Entries Ever Used	The largest number of VLANs that have been active on this switch since the last reboot.
Static VLAN Entries	The number of presently active VLAN entries on this switch that have been created statically.
Dynamic VLAN Entries	The number of presently active VLAN entries on this switch that have been created by GVRP registration.
VLAN Deletes	The number of VLANs on this switch that have been created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

show mac-addr-table

This command displays the forwarding database entries. These entries are used by the transparent bridging function to determine how to forward a received frame.

Enter `all` or no parameter to display the entire table. Enter a MAC Address and VLAN ID to display the table entry for the requested MAC address on the specified VLAN. Enter the `count` parameter to view summary information about the

forwarding database table. Use the *interface <slot/port>* parameter to view MAC addresses on a specific interface. Use the *vlan <vlan_id>* parameter to display information about MAC addresses on a specified VLAN.

Format **show mac-addr-table** *[{<macaddr> <vlan_id> | all | count | interface <slot/port> | vlan <vlan_id>}]*

Mode Privileged EXEC

The following information displays if you do not enter a parameter, the keyword all, or the MAC address and VLAN ID. If you enter *vlan <vlan_id>*, only the Mac Address, Interface, and Status fields appear.

Term	*Definition*
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
Interface	The port through which this address was learned.
Interface Index	This object indicates the ifIndex of the interface table entry associated with this port.
Status	The status of this entry. The meanings of the values are: • *Static*—The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned. • *Learned*—The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use. • *Management*—The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 0/1. and is currently used when enabling VLANs for routing. • *Self*—The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address). • *GMRP Learned*—The value of the corresponding was learned via GMRP and applies to Multicast. • *Other*—The value of the corresponding instance does not fall into one of the other categories.

If you enter the *interface <slot/port>* parameter, in addition to the MAC Address and Status fields, the following field appears:

Term	*Definition*
VLAN ID	The VLAN on which the MAC address was learned.

The following information displays if you enter the *count* parameter:

Term	*Definition*
Dynamic Address count	Number of MAC addresses in the forwarding database that were automatically learned.
Static Address (User-defined) count	Number of MAC addresses in the forwarding database that were manually entered by a user.
Total MAC Addresses in use	Number of MAC addresses currently in the forwarding database.
Total MAC Addresses available	Number of MAC addresses the forwarding database can handle.

show process cpu

This command provides the percentage utilization of the CPU by different tasks.

Note: It is not necessarily the traffic to the CPU, but different tasks that keep the CPU busy.

Format	`show process cpu`
Mode	Privileged EXEC

The following shows example CLI display output for the command for VxWorks.

```
(DWS-4026) #show process cpu

Memory Utilization Report

status      bytes
------ ----------
  free  101133744
 alloc  134315888

CPU Utilization:
 PID     Name                    5 Sec    1 Min    5 Min
-------------------------------------------------------
 1f9e520 tNetTask                0.00%    0.00%    0.04%
 218a770 ipnetd                  0.00%    0.06%    0.10%
 2280880 bcmL2X.0                0.40%    0.70%    0.99%
 22b1940 bcmCNTR.0               0.00%    0.38%    0.35%
 22c9070 bcmTX                   0.00%    0.00%    0.01%
 27e2e30 bcmLINK.0               1.60%    1.50%    1.33%
 27f1eb8 bcmRX                   0.00%    0.15%    0.10%
 29a23f8 cpuUtilMonitorTask      0.40%    0.40%    0.40%
 2ac8948 osapiMonTask            0.00%    0.10%    0.06%
 2e75f30 webJavaTask             0.40%    0.21%    0.18%
 2f23120 tEmWeb                  0.00%    0.06%    0.02%
 2f5f760 dtlTask                 0.00%    0.00%    0.09%
 2f68d58 dtlAddrTask             0.00%    0.06%    0.02%
 30780a8 hapiRxTask              0.00%    0.06%    0.30%
 32005c0 poe_read                0.00%    0.00%    0.15%
 3209b58 poe_monitor             0.00%    0.06%    0.07%
 3b0ead8 RMONTask                1.20%    0.26%    0.29%
 57a42d8 ipMapForwardingTask     0.00%    0.00%    0.09%
 8c95698 wlanPeerTxRxTask        0.00%    0.10%    0.30%
 8ca1250 wlanDiscoverTask        0.00%    0.06%    0.01%
-------------------------------------------------------

 Total CPU Utilization           4.00%    4.16%    4.90%
```

show running-config

Use this command to display or capture the current setting of different protocol packages supported on the switch. This command displays or captures commands with settings and configurations that differ from the default value. To display or capture the commands with settings and configurations that are equal to the default value, include the *[all]* option.

Note: Show running-config does not display the User Password, even if you set one different from the default.

The output is displayed in script format, which can be used to configure another switch with the same configuration. If the optional *<scriptname>* is provided with a file name extension of ".scr", the output is redirected to a script file.

Note: If you issue the **show running-config** command from a serial connection, access to the switch through remote connections (such as Telnet) is suspended while the output is being generated and displayed.

Note: If you use a text-based configuration file, the **show running-config** command will only display configured physical interfaces, i.e. if any interface only contains the default configuration, that interface will be skipped from the **show running-config** command output. This is true for any configuration mode that contains nothing but default configuration. That is, the command to enter a particular config mode, followed immediately by its exit command, are both omitted from the **show running-config** command output (and hence from the startup-config file when the system configuration is saved.)

Format	**show running-config** *[all | <scriptname>]*
Mode	Privileged EXEC

There are three command modes:

1. <cr> — Press **Enter** to execute the command.
2. <scriptname> — Script filename for writing active configuration.
3. all — Show all the running configuration on the switch.

Example: The following shows example CLI display captive portal output.

```
(DWS-4026) #show running config [all]
captive-portal
enable
authentication timeout 300
http port 8080
https port 60000
statistics interval 120
no trapflags client-auth-failure
no trapflags client-connect
no trapflags client-db-full
no trapflags client-disconnect
user group 1
user group 1 name "Default"
configuration 1
name "Default"
enable
protocol https
verification guest
no redirect
session-timeout 0
idle-timeout 0
max-bandwidth-up 0
max-bandwidth-down 0
--More-- or (q)uit

max-input-octets 0
max-output-octets 0
max-total-octets 0
interface 8/1
separator-color "#B70024"
background-color "#BFBFBF"
foreground-color "#999999"
locale 1
code "en"
account-image "login_key.jpg"
account-label
0045006E00740065007200200079006F007500720020005500730065007200 6E0061006D0065002E
```



```
accept-msg
004500720072006F0072003A00200059006F00750020006D0075007300740020006100630063006B006E006F007
7006C0065006400670065002000740068006500200041006300630065007000740061006E00630065002000
550073006500200050006F006C00690063007900200062006500660066006F00720065002000063006F006E006E0
06500630074006900 6E00670021
accept-text
004300680065006300 6B0020006800650072006500200074006F00200069006E0064006900630061 0074006
5002000740068006100740020007 9006F0075002000680061007600650020007200650061006400200061 00
6E00640020006100630063006500700074006500640020007400680065002000410063006300650070 00740
061006E006300650020005500730065002000 50006F006C006900630079002E
no aup-text
aup-text
004100630063006500700074006100 6E006300650020005500730065002000 50006F006C006900630079
button-label 0043006F006E006E00650063 0074
branding-image "BRCM_logo.gif"
browser-title 004300610070007400690076006500200050006F007200740061006C
denied-msg
004500720072006F0072003A00200049006E00760061006C006900640020004300720065006400650006E007
400690061006C0073002C00200070006C006500610073006500200074007200790020006100670061006900
6E0021
font-list "arial, sans-serif"
no instructional-text
instructional-text
0054006F00200073007400610072007400200075007300690006E006700200074006800690073002000073006
50072007600690063006500 2C00200065006E0074006500720020007 9006F0075007200200063007200650 0
640065006E007400690061006C00730020006100 6E006400200063006C00690063006B002000740068006 50
0200043006F006E006E00650063007400200062007500740074006F006E002E
link 00280045006E0067006C0069007300680029
password-label 00500061007300730077006F00720064

--More-- or (q)uit
resource-msg
004500720072006F0072003A0020004C0069006D006900740065006400200052006500730 06F00750072006
300650073002C00200070006C006500610073006500200072006500630006F006E006E00650063007400 2000
61006E0064002000740072007900200061006700610069006E0020006C00610074006500720021
title-text
00570065006C0063006F006D00650020 0074006F002000740068006500200057006900720065006C0065007
30073 0020004E006500740077006F0072006B
timeout-msg
004500720072006F0072003A00200054 0069006D006500640020004F00750074002C00200070006C0065006
10073006500200072006500630006F006E006E006500630074002000610006E006400200074007200790 02000
61006700610069006E0021
user-label 0055007300650072006E0061006D0065
welcome-title 0043006F006E0067007200610074007500 6C006100740069006F006E00730021
no welcome-text
welcome-text
0059006F0075002000610072006500200006E006F00770020006100750074006800 6F00720069007A0065006
4002000 61006E00640020 0063006F006E006E006500630074006500640020 0074006F00200074006800650 0
20006E006500740077006F0072006B002E
wip-msg
0043006F006E006E0065006300740069006E0067002C00200070006C0065006100730065002000620065002
0007000610074006900650006E0074
exit
exit
exit
```

show sysinfo

This command displays switch information.

Format	`show sysinfo`
Mode	Privileged EXEC

Term	*Definition*
Switch Description	Text used to identify this switch.
System Name	Name used to identify the switch.The factory default is blank. To configure the system name, see "snmp-server" on page 496.
System Location	Text used to identify the location of the switch. The factory default is blank. To configure the system location, see "snmp-server" on page 496.
System Contact	Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see "snmp-server" on page 496.
System ObjectID	The base object ID for the switch's enterprise MIB.
System Up Time	The time in days, hours and minutes since the last switch reboot.
MIBs Supported	A list of MIBs supported by this agent.

show tech-support

Use the **`show tech-support`** command to display system and configuration information when you contact technical support. The output of the **`show tech-support`** command combines the output of the following commands:

- **`show version`**
- **`show sysinfo`**
- **`show port all`**
- show isdp neighbors
- **`show logging`**
- **`show event log`**
- **`show logging buffered`**
- **`show trap log`**
- **`show running config`**

Format	`show tech-support`
Mode	Privileged EXEC

terminal length

Use this command to set the number of lines of output to be displayed on the screen, i.e. pagination, for the **`show running-config`** and **`show running-config all`** commands. The terminal length size is either zero or a number in the range of 5 to 48. After the user-configured number of lines is displayed in one page, the system prompts the user for `--More-- or (q)uit. Press q or Q to quit, or press any key to display the next set of <5-48> lines. The`

command **terminal length 0** disables pagination and, as a result, the output of the **show running-config** command is displayed immediately.

Default	24 lines per page
Format	**terminal length** <0|*5-48*>
Mode	Privileged EXEC

no terminal length

Use this command to set the terminal length to the default value.

show terminal length

Use this command to display the value of the user-configured terminal length size.

Format	**show terminal length**
Mode	Privileged EXEC

nvram size

Use this command to display NVRAM size information.

Format	**show nvram-size**
Mode	Global Config

The output shows the NVRAM size in bytes, the bytes used, and the bytes available.

LOGGING COMMANDS

This section describes the commands you use to configure system logging, and to view logs and the logging settings.

logging buffered

This command enables logging to an in-memory log that keeps up to 128 logs.

Default	disabled; critical when enabled
Format	`logging buffered`
Mode	Global Config

no logging buffered

This command disables logging to in-memory log.

Format	`no logging buffered`
Mode	Global Config

logging buffered wrap

This command enables wrapping of in-memory logging when the log file reaches full capacity. Otherwise when the log file reaches full capacity, logging stops.

Default	enabled
Format	`logging buffered wrap`
Mode	Privileged EXEC

no logging buffered wrap

This command disables wrapping of in-memory logging and configures logging to stop when the log file capacity is full.

Format	`no logging buffered wrap`
Mode	Privileged EXEC

logging cli-command

This command enables the CLI command logging feature, which enables the Unified Switch software to log all CLI commands issued on the system.

Default	enabled
Format	`logging cli-command`
Mode	Global Config

no logging cli-command

This command disables the CLI command Logging feature.

Format	**no logging cli-command**
Mode	Global Config

logging console

This command enables logging to the console. You can specify the *<severitylevel>* value as either an integer from 0 to 7 or symbolically through one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

Default	disabled; critical when enabled
Format	**logging console** *[severitylevel]*
Mode	Global Config

no logging console

This command disables logging to the console.

Format	**no logging console**
Mode	Global Config

logging host

This command enables logging to a host. You can configure up to eight hosts. The *<ipaddr|hostname>* is the IP address of the logging host. The *<addresstype>* indicates the type of address (ipv4 or dns) being passed. The *<port>* value is a port number from 1 to 65535. You can specify the *<severitylevel>* value as either an integer from 0 to 7 or symbolically through one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

Default	• port—514 • level—critical (2)
Format	**logging host** *<ipaddr|hostname> <addresstype> [<port>][<severitylevel>]*
Mode	Global Config

logging host remove

This command disables logging to host. See “show logging hosts” on page 429 for a list of host indexes.

Format	**logging host remove** *<hostindex>*
Mode	Global Config

logging port

This command sets the local port number of the LOG client for logging messages. The *<portid>* can be in the range from 1 to 65535.

Default	514
Format	**logging port** *<portid>*
Mode	Global Config

no logging port

This command resets the local logging port to the default.

Format	**no logging port**
Mode	Global Config

logging syslog

This command enables syslog logging. The *<portid>* parameter is an integer with a range of 1-65535.

Default	disabled
Format	**logging syslog** *[port <portid>]*
Mode	Global Config

no logging syslog

This command disables syslog logging.

Format	**no logging syslog**
Mode	Global Config

show logging

This command displays logging configuration information.

Format	**show logging**
Mode	Privileged EXEC

Term	*Definition*
Logging Client Local Port	Port on the collector/relay to which syslog messages are sent.
CLI Command Logging	Shows whether CLI Command logging is enabled.
Console Logging	Shows whether console logging is enabled.
Console Logging Severity Filter	The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.
Buffered Logging	Shows whether buffered logging is enabled.

Term	*Definition*
Syslog Logging	Shows whether syslog logging is enabled.
Log Messages Received	Number of messages received by the log process. This includes messages that are dropped or ignored.
Log Messages Dropped	Number of messages that could not be processed due to error or lack of resources.
Log Messages Relayed	Number of messages sent to the collector/relay.

show logging buffered

This command displays buffered logging (system startup and system operation logs).

Format `show logging buffered`

Mode Privileged EXEC

Term	*Definition*
Buffered (In-Memory) Logging	Shows whether the In-Memory log is enabled or disabled.
Buffered Logging Wrapping Behavior	The behavior of the In Memory log when faced with a log full situation.
Buffered Log Count	The count of valid entries in the buffered log.

show logging hosts

This command displays all configured logging hosts. The *<unit>* is the switch identifier and has a range of 1-8.

Format `show logging hosts` *<unit>*

Mode Privileged EXEC

Term	*Definition*
Host Index	(Used for deleting hosts.)
IP Address / Hostname	IP address or hostname of the logging host.
Severity Level	The minimum severity to log to the specified address. The possible values are emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).
Port	The server port number, which is the port on the local host from which syslog messages are sent.
Host Status	The state of logging to configured syslog hosts. If the status is disable, no logging occurs.

show logging traplogs

This command displays SNMP trap events and statistics.

Format `show logging traplogs`

Mode Privileged EXEC

Term	*Definition*
Number of Traps Since Last Reset	The number of traps since the last boot.
Trap Log Capacity	The number of traps the system can retain.
Number of Traps Since Log Last Viewed	The number of new traps since the command was last executed.
Log	The log number.
System Time Up	How long the system had been running at the time the trap was sent.
Trap	The text of the trap message.

SYSTEM UTILITY AND CLEAR COMMANDS

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

traceroute

Use the **traceroute** command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. Traceroute continues to provide a synchronous response when initiated from the CLI.

Default
- count: 3 probes
- interval: 3 seconds
- size: 0 bytes
- port: 33434
- maxTtl: 30 hops
- maxFail: 5 probes
- initTtl: 1 hop
-

Format **traceroute** <*ipaddr*|*hostname*> [**initTtl** <*initTtl*>] [**maxTtl** <*maxTtl*>] [**maxFail** <*maxFail*>] [**interval** <*interval*>] [**count** <*count*>] [**port** <*port*>] [**size** <*size*>]

Mode Privileged EXEC

Using the options described below, you can specify the initial and maximum time-to-live (TTL) in probe packets, the maximum number of failures before termination, the number of probes sent for each TTL, and the size of each probe.

Parameter	*Description*
ipaddr|**hostname**	The *ipaddr* value should be a valid IP address. The *hostname* value should be a valid hostname.
initTtl	Use initTtl to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 0 to 255.
maxTtl	Use maxTtl to specify the maximum TTL. Range is 1 to 255.
maxFail	Use maxFail to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.
interval	Use interval to specify the time between probes, in seconds. Range is 1 to 60 seconds.

Parameter	*Description*
count	Use the optional `count` parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.
port	Use the optional `port` parameter to specify destination UDP port of the probe. This should be an unused port on the remote destination system. Range is 1 to 65535.
size	Use the optional `size` parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.

The following are examples of the CLI command.

Example: traceroute Success:

```
(DWS-4026) # traceroute 10.240.10.115 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3
port 33434 size 43
 Traceroute to 10.240.10.115 ,4 hops max 43 byte packets:
1 10.240.4.1   708 msec     41 msec     11 msec
2 10.240.10.115   0 msec     0 msec     0 msec

Hop Count = 1 Last TTL = 2 Test attempt = 6 Test Success = 6
```

Example: traceroute Failure:

```
(DWS-4026) # traceroute 10.40.1.1 initTtl 1 maxFail 0 interval 1 count 3
port 33434 size 43
Traceroute to 10.40.1.1 ,30 hops max 43 byte packets:
1 10.240.4.1   19 msec     18 msec     9 msec
2 10.240.1.252   0 msec     0 msec     1 msec
3 172.31.0.9   277 msec     276 msec     277 msec
4 10.254.1.1   289 msec     327 msec     282 msec
5 10.254.21.2   287 msec     293 msec     296 msec
6 192.168.76.2   290 msec     291 msec     289 msec
7 0.0.0.0   0 msec *
Hop Count = 6 Last TTL = 7 Test attempt = 19 Test Success = 18
```

clear config

This command resets the configuration to the factory defaults without powering off the switch. When you issue this command, a prompt appears to confirm that the reset should proceed. When you enter **y**, you automatically reset the current configuration on the switch to the default values. It does not reset the switch.

Format	**`clear config`**
Mode	Privileged EXEC

clear counters

This command clears the statistics for a specified *<slot/port>,* for all the ports, or for the entire switch based upon the argument.

Format	**`clear counters`** *{<slot/port> | all}*
Mode	Privileged EXEC

clear igmpsnooping

This command clears the tables managed by the IGMP Snooping function and attempts to delete these entries from the Multicast Forwarding Database.

Format	`clear igmpsnooping`
Mode	Privileged EXEC

clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

Format	`clear pass`
Mode	Privileged EXEC

clear port-channel

This command clears all port-channels (LAGs).

Format	`clear port-channel`
Mode	Privileged EXEC

clear traplog

This command clears the trap log.

Format	`clear traplog`
Mode	Privileged EXEC

clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format	`clear vlan`
Mode	Privileged EXEC

enable passwd

This command prompts you to change the Privileged EXEC password. Passwords are a maximum of 64 alphanumeric characters. The password is case sensitive.

Format	`enable passwd`
Mode	Privileged EXEC

enable passwd encrypted

This command allows the administrator to transfer the enable password between devices without having to know the password. The *<password>* parameter must be exactly 128 hexadecimal characters.

Format	**enable passwd encrypted** *<password>*
Mode	Privileged EXEC

logout

This command closes the current telnet connection or resets the current serial connection.

Note: Save configuration changes before logging out.

Format	**logout**
Modes	• Privileged EXEC • User EXEC

ping

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI and Web interfaces.

Default	• The default count is 1. • The default interval is 3 seconds. • The default size is 0 bytes.
Format	**ping** *<ipaddress|hostname>* **[count** *<count>***] [interval** *<interval>***] [size** *<size>***]**
Modes	• Privileged EXEC • User EXEC

Using the options described below, you can specify the number and size of Echo Requests and the interval between Echo Requests.

Parameter	*Description*
count	Use the **count** parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the *<ip-address>* field. The range for *<count>* is 1 to 15 requests.
interval	Use the **interval** parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.
size	Use the **size** parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.

The following are examples of the CLI command.

Example: ping success:

```
(DWS-4026) #ping 10.254.2.160 count 3 interval 1 size 255
Pinging 10.254.2.160 with 255 bytes of data:
```

```
Received response for icmp_seq = 0. time = 275268 usec
Received response for icmp_seq = 1. time = 274009 usec
Received response for icmp_seq = 2. time = 279459 usec

----10.254.2.160 PING statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 274/279/276
```

Example: ping failure:

In Case of Unreachable Destination:

```
(DWS-4026) # ping 192.168.254.222 count 3 interval 1 size 255
Pinging 192.168.254.222 with 255 bytes of data:
Received Response: Unreachable Destination
Received Response :Unreachable Destination
Received Response :Unreachable Destination
----192.168.254.222  PING statistics----
3 packets transmitted,3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

In Case Of Request TimedOut:

```
(DWS-4026) # ping 1.1.1.1 count 1 interval 3
Pinging 1.1.1.1 with 0 bytes of data:

----1.1.1.1 PING statistics----
1 packets transmitted,0 packets received, 100% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

quit

This command closes the current telnet connection or resets the current serial connection. The system asks you whether to save configuration changes before quitting.

Format	**quit**
Modes	• Privileged EXEC • User EXEC

reload

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. The LEDs on the switch indicate a successful reset.

Format	**reload**
Mode	Privileged EXEC

copy

The **copy** command uploads and downloads files to and from the switch. You can also use the copy command to manage the dual images (*image1* and *image2*) on the file system. Upload and download files from a server by using TFTP or

Xmodem. SFTP and SCP are available as additional transfer methods if the software package supports secure management.

Format **copy** *<source> <destination>*

Mode Privileged EXEC

Replace the *<source>* and *<destination>* parameters with the options in Table 11. For the *<url>* source or destination, use one of the following values:

{xmodem | tftp://<ipaddr|hostname>/<filepath>/<filename> [noval] | sftp|scp://<username>@<ipaddr>|<ipv6address>|<filepath>|<filename>}

For TFTP, SFTP and SCP, the *<ipaddr|hostname>* parameter is the IP address or host name of the server, *<filepath>* is the path to the file, and *<filename>* is the name of the file you want to upload or download. For SFTP and SCP, the *<username>* parameter is the username for logging into the remote server via SSH.

Table 11: Copy Parameters

Source	*Destination*	*Description*
nvram:backup-config	*nvram:startup-config*	Copies the backup configuration to the startup configuration.
nvram:clibanner	*<url>*	Copies the CLI banner to a server.
nvram:errorlog	*<url>*	Copies the error log file to a server.
nvram:fastpath.cfg	*<url>*	Uploads the binary config file to a server.
nvram:log	*<url>*	Copies the log file to a server.
nvram:script <scriptname>	*<url>*	Copies a specified configuration script file to a server.
nvram:startup-config	*nvram:backup-config*	Copies the startup configuration to the backup configuration.
nvram:startup-config	*<url>*	Copies the startup configuration to a server.
nvram:traplog	*<url>*	Copies the trap log file to a server.
system:running-config	*nvram:startup-config*	Saves the running configuration to nvram.
<url>	*nvram:clibanner*	Downloads the CLI banner to the system.
<url>	*nvram:fastpath.cfg*	Downloads the binary config file to the system.
<url>	*nvram:script <destfilename>*	Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. In case of any error, the command lists all the lines at the end of the validation process and prompts you to confirm before copying the script file.
<url>	*nvram:script <destfilename> noval*	When you use this option, the copy command will not validate the downloaded script file. An example of the CLI command follows:
`(DWS-4026) #copy tftp://1.1.1.1/file.scr nvram:script file.scr noval`		
<url>	*nvram:sshkey-dsa*	Downloads an SSH key file. For more information, see "Secure Shell Commands" on page 481.
<url>	*nvram:sshkey-rsa1*	Downloads an SSH key file.
<url>	*nvram:sshkey-rsa2*	Downloads an SSH key file.
<url>	*nvram:sslpem-dhweak*	Downloads an HTTP secure-server certificate.
<url>	*nvram:sslpem-dhstrong*	Downloads an HTTP secure-server certificate.

Table 11: Copy Parameters (Cont.)

Source	Destination	Description
<url>	*nvram:sslpem-root*	Downloads an HTTP secure-server certificate. For more information, see "Hypertext Transfer Protocol Commands" on page 485.
<url>	*nvram:sslpem-server*	Downloads an HTTP secure-server certificate.
<url>	*nvram:startup-config*	Downloads the startup configuration file to the system.
<url>	*nvram:system-image*	Downloads a code image to the system.
<url>	*{image1 | image2}*	Download an image from the remote server to either image.
{image1 | image2}	*<url>*	Upload either image to the remote server.
image1	*image2*	Copy **image1** to **image2**.
image2	*image1*	Copy **image2** to **image1**.

SNTP AND CLOCK COMMANDS

This section describes the commands you use to automatically configure the Simple Network Time Protocol (SNTP) commands, and the time zone and daylight savings time commands.

SNTP COMMANDS

sntp broadcast client poll-interval

This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where *<poll-interval>* can be a value from 6 to 16.

Default 6

Format **sntp broadcast client poll-interval** *<poll-interval>*

Mode Global Config

no sntp broadcast client poll-interval

This command resets the poll interval for SNTP broadcast client back to the default value.

Format **no sntp broadcast client poll-interval**

Mode Global Config

sntp client mode

This command enables Simple Network Time Protocol (SNTP) client mode and may set the mode to either broadcast or unicast.

Default disabled

Format **sntp client mode** *[broadcast | unicast]*

Mode Global Config

no sntp client mode

This command disables Simple Network Time Protocol (SNTP) client mode.

Format **no sntp client mode**
Mode Global Config

sntp client port

This command sets the SNTP client port id to a value from 1-65535.

Default 123
Format **sntp client port** *<portid>*
Mode Global Config

no sntp client port

This command resets the SNTP client port back to its default value.

Format **no sntp client port**
Mode Global Config

sntp unicast client poll-interval

This command sets the poll interval for SNTP unicast clients in seconds as a power of two where <poll-interval> can be a value from 6 to 16.

Default 6
Format **sntp unicast client poll-interval** *<poll-interval>*
Mode Global Config

no sntp unicast client poll-interval

This command resets the poll interval for SNTP unicast clients to its default value.

Format **no sntp unicast client poll-interval**
Mode Global Config

sntp unicast client poll-timeout

This command will set the poll timeout for SNTP unicast clients in seconds to a value from 1-30.

Default 5
Format **sntp unicast client poll-timeout** *<poll-timeout>*
Mode Global Config

no sntp unicast client poll-timeout

This command will reset the poll timeout for SNTP unicast clients to its default value.

Format	**no sntp unicast client poll-timeout**
Mode	Global Config

sntp unicast client poll-retry

This command will set the poll retry for SNTP unicast clients to a value from 0 to 10.

Default	1
Format	**sntp unicast client poll-retry** *<poll-retry>*
Mode	Global Config

no sntp unicast client poll-retry

This command will reset the poll retry for SNTP unicast clients to its default value.

Format	**no sntp unicast client poll-retry**
Mode	Global Config

sntp multicast client poll-interval

This command will set the poll interval for SNTP multicast clients in seconds as a power of two where *<poll-interval>* can be a value from 6 to 16.

Default	6
Format	**sntp multicast client poll-interval** *<poll-interval>*
Mode	Global Config

no sntp multicast client poll-interval

This command resets the poll interval for SNTP multicast clients to its default value.

Format	**no sntp multicast client poll-interval**
Mode	Global Config

sntp server

This command configures an SNTP server (a maximum of three). The optional priority can be a value of 1-3, the version a value of 1-4, and the port id a value of 1-65535.

Format	**sntp server** *<ipaddress|hostname> [<priority> [<version> [<portid>]]]*
Mode	Global Config

no sntp server

This command deletes an server from the configured SNTP servers.

Format **no sntp server remove** *<ipaddress|hostname>*

Mode Global Config

show sntp

This command is used to display SNTP settings and status.

Format **show sntp**

Mode Privileged EXEC

Term	*Definition*
Last Update Time	Time of last clock update.
Last Attempt Time	Time of last transmit query (in unicast mode).
Last Attempt Status	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
Broadcast Count	Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.

show sntp client

This command is used to display SNTP client settings.

Format **show sntp client**

Mode Privileged EXEC

Term	*Definition*
Client Supported Modes	Supported SNTP Modes (Broadcast or Unicast).
SNTP Version	The highest SNTP version the client supports.
Port	SNTP Client Port.
Client Mode	Configured SNTP Client Mode.

show sntp server

This command is used to display SNTP server settings and configured servers.

Format **show sntp server**

Mode Privileged EXEC

Term	*Definition*
Server IP Address / Hostname	IP address or hostname of configured SNTP Server.
Server Type	Address Type of Server.
Server Stratum	Claimed stratum of the server for the last received valid packet.
Server Reference ID	Reference clock identifier of the server for the last received valid packet.
Server Mode	SNTP Server mode.
Server Maximum Entries	Total number of SNTP Servers allowed.
Server Current Entries	Total number of SNTP configured.

For each configured server:

Term	*Definition*
IP Address / Hostname	IP address or hostname of configured SNTP Server.
Address Type	Address Type of configured SNTP server.
Priority	IP priority type of the configured server.
Version	SNTP Version number of the server. The protocol version used to query the server in unicast mode.
Port	Server Port Number.
Last Attempt Time	Last server attempt time for the specified server.
Last Update Status	Last server attempt status for the server.
Total Unicast Requests	Number of requests to the server.
Failed Unicast Requests	Number of failed requests from server.

TIME ZONE AND DAYLIGHT SAVINGS TIME COMMANDS

clock timezone

This command configures the timezone by specifying an offset from the Coordinated Universal Time (UTC), which is retreived from the SNTP server.

Default none

Format **clock timezone offset** *<offset>* **minutes** *<offset>* **zone** *<offset>*

Mode Global Config

Term	*Definition*
offset	Replace *<offset>* with the number of hours your time zone differs from the UTC time, in the range –12 to 13. A negative value indicates that the time zone later than the UTC, and a positive value indicates a time zone that is earlier than the UTC.

Term	*Definition*
minutes	Replace *<minutes>* with the number of minutes your time zone differs from the UTC, in addition to the offset, in the range -59 to +59.
zone *<zone>*	Replace *<zone>* with an acronym for the time zone.

Example: The following example configures the time zone to 5 hours and 30 minutes earlier than UTC, and names it *IST*.

```
clock timezone offset 5 minutes 30 date zone IST
```

clock summer-time date

This command configures daylight savings time parameters, which adjust the time by a specified amount between the specified dates and times

Default none

Format **clock summer-time date** *<starting month dd yyyy hh:mm> <ending month dd yyyy hh:mm>* offset *<offset>* zone *<zone>*

Mode Global Config

Replace the values as follows:

Term	*Definition*
month	Replace *<starting month>* and *<ending month>* with the first three letters of the month (i.e., *jan*, *feb*, *mar*, etc.). Do not enter the words *starting* or *ending*.
dd	Day of month in the range 1 to 31.
yyyy	Year in four characters
hh	Hours in the range 0 to 24
mm	Minutes in the range 0 to 59
offset *<offset>*	Replace *<offset>* with the amount of time the clock is moved forward on the starting date and backward on the ending date.
zone *<zone>*	Replace *<zone>* with an acronym for the time zone during daylight savings time.

Example: The following example configures daylight savings time to begin at midnight on March 8, 2009 at 2:00 AM, and end on November 1, 2009 at 2:00 AM. It sets the clock back 1 hour and names the time zone PDT (e.g., Pacific Daylight Time)

```
clock summer-time date mar 8 2009 02:00 nov 1 2009 2:00 offset 60 zone PDT
```

DHCP SERVER COMMANDS

This section describes the commands you to configure the DHCP server settings for the switch. DHCP uses UDP as its transport protocol and supports a number of features that facilitate in administration address allocations.

ip dhcp pool

This command configures a DHCP address pool name on a DHCP server and enters DHCP pool configuration mode.

Default	none
Format	**ip dhcp pool** *<name>*
Mode	Global Config

no ip dhcp pool

This command removes the DHCP address pool. The name should be previously configured pool name.

Format	**no ip dhcp pool** *<name>*
Mode	Global Config

client-identifier

This command specifies the unique identifier for a DHCP client. Unique-identifier is a valid notation in hexadecimal format. In some systems, such as Microsoft DHCP clients, the client identifier is required instead of hardware addresses. The unique-identifier is a concatenation of the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address c819.2488.f177 is 01c8.1924.88f1.77 where 01 represents the Ethernet media type. For more information, refer to the “Address Resolution Protocol Parameters” section of RFC 1700, Assigned Numbers for a list of media type codes.

Default	none
Format	**client-identifier** *<uniqueidentifier>*
Mode	DHCP Pool Config

no client-identifier

This command deletes the client identifier.

Format	**no client-identifier**
Mode	DHCP Pool Config

client-name

This command specifies the name for a DHCP client. Name is a string consisting of standard ASCII characters.

Default	none
Format	**client-name** *<name>*
Mode	DHCP Pool Config

no client-name

This command removes the client name.

Format	**no client-name**
Mode	DHCP Pool Config

default-router

This command specifies the default router list for a DHCP client. {*address1, address2… address8*} are valid IP addresses, each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none
Format	**default-router** *<address1> [<address2>....<address8>]*
Mode	DHCP Pool Config

no default-router

This command removes the default router list.

Format	**no default-router**
Mode	DHCP Pool Config

dns-server

This command specifies the DNS servers available to a DHCP client. Address parameters are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none
Format	**dns-server** *<address1> [<address2>....<address8>]*
Mode	DHCP Pool Config

no dns-server

This command removes the DNS Server list.

Format	**no dns-server**
Mode	DHCP Pool Config

hardware-address

This command specifies the hardware address of a DHCP client. Hardware-address is the MAC address of the hardware platform of the client consisting of 6 bytes in dotted hexadecimal format. Type indicates the protocol of the hardware platform. It is 1 for 10 MB Ethernet and 6 for IEEE 802.

Default	ethernet
Format	**hardware-address** *<hardwareaddress> <type>*
Mode	DHCP Pool Config

no hardware-address

This command removes the hardware address of the DHCP client.

Format	**no hardware-address**
Mode	DHCP Pool Config

host

This command specifies the IP address and network mask for a manual binding to a DHCP client. Address and Mask are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. The prefix-length is an integer from 0 to 32.

Default	none
Format	**host** *<address> [{<mask> | <prefix-length>}]*
Mode	DHCP Pool Config

no host

This command removes the IP address of the DHCP client.

Format	**no host**
Mode	DHCP Pool Config

lease

This command configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client. The overall lease time should be between 1-86400 minutes. If you specify *infinite*, the lease is set for 60 days. You can also specify a lease duration. *Days* is an integer from 0 to 59. *Hours* is an integer from 0 to 23. *Minutes* is an integer from 0 to 59.

Default	1 (day)
Format	**lease** *[{<days> [<hours>] [<minutes>] | infinite}]*
Mode	DHCP Pool Config

no lease

This command restores the default value of the lease time for DHCP Server.

Format	**no lease**
Mode	DHCP Pool Config

network (DHCP Pool Config)

Use this command to configure the subnet number and mask for a DHCP address pool on the server. Network-number is a valid IP address, made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. Mask is the IP subnet mask for the specified address pool. The prefix-length is an integer from 0 to 32.

Default	none
Format	**network** *<networknumber> [{<mask> | <prefixlength>}]*
Mode	DHCP Pool Config

no network

This command removes the subnet number and mask.

Format	**no network**
Mode	DHCP Pool Config

bootfile

The command specifies the name of the default boot image for a DHCP client. The *<filename>* specifies the boot image file.

Format	**bootfile** *<filename>*
Mode	DHCP Pool Config

no bootfile

This command deletes the boot image name.

Format	**no bootfile**
Mode	DHCP Pool Config

domain-name

This command specifies the domain name for a DHCP client. The *<domain>* specifies the domain name string of the client.

Default	none
Format	**domain-name** *<domain>*
Mode	DHCP Pool Config

no domain-name

This command removes the domain name.

Format	**no domain-name**
Mode	DHCP Pool Config

netbios-name-server

This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to DHCP clients.

One IP address is required, although one can specify up to eight addresses in one command line. Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Default	none
Format	**netbios-name-server** *<address> [<address2>...<address8>]*
Mode	DHCP Pool Config

no netbios-name-server

This command removes the NetBIOS name server list.

Format	**no netbios-name-server**
Mode	DHCP Pool Config

netbios-node-type

The command configures the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients. Valid types are:

- b-node—Broadcast
- p-node—Peer-to-peer
- m-node—Mixed
- h-node—Hybrid (recommended)

Default	none
Format	**netbios-node-type** *<type>*
Mode	DHCP Pool Config

no netbios-node-type

This command removes the NetBIOS node Type.

Format	**no netbios-node-type**
Mode	DHCP Pool Config

next-server

This command configures the next server in the boot process of a DHCP client.The *<address>* parameter is the IP address of the next server in the boot process, which is typically a TFTP server.

Default	inbound interface helper addresses
Format	**next-server** *<address>*
Mode	DHCP Pool Config

no next-server

This command removes the boot server list.

Format	**no next-server**
Mode	DHCP Pool Config

option

The **option** command configures DHCP Server options. The *<code>* parameter specifies the DHCP option code and ranges from 1-254. The *<ascii string>* parameter specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks. The *hex <string>* parameter specifies hexadecimal data. In hexadecimal, character strings are two hexadecimal digits. You can separate each byte by a period (for example, a3.4f.22.0c), colon (for example, a3:4f:22:0c), or white space (for example, a3 4f 22 0c).

Default	none
Format	**option** *<code> {ascii string | hex <string1> [<string2>...<string8>] | ip <address1> [<address2>...<address8>]}*
Mode	DHCP Pool Config

no option

This command removes the DHCP Server options. The *<code>* parameter specifies the DHCP option code.

Format	**no option** *<code>*
Mode	DHCP Pool Config

ip dhcp excluded-address

This command specifies the IP addresses that a DHCP server should not assign to DHCP clients. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none
Format	**ip dhcp excluded-address** *<lowaddress> [highaddress]*
Mode	Global Config

no ip dhcp excluded-address

This command removes the excluded IP addresses for a DHCP client. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Format	**no ip dhcp excluded-address** *<lowaddress> [highaddress]*
Mode	Global Config

ip dhcp ping packets

Use this command to specify the number, in a range from 2-10, of packets a DHCP server sends to a pool address as part of a ping operation. By default the number of packets sent to a pool address is 2, which is the smallest allowed number when sending packets. Setting the number of packets to 0 disables this command.

Default 2
Format **ip dhcp ping packets** *<0,2-10>*
Mode Global Config

no ip dhcp ping packets

This command prevents the server from pinging pool addresses and sets the number of packets to 0.

Default 0
Format **no ip dhcp ping packets**
Mode Global Config

service dhcp

This command enables the DHCP server.

Default disabled
Format **service dhcp**
Mode Global Config

no service dhcp

This command disables the DHCP server.

Format **no service dhcp**
Mode Global Config

ip dhcp bootp automatic

This command enables the allocation of the addresses to the bootp client. The addresses are from the automatic address pool.

Default disabled
Format **ip dhcp bootp automatic**
Mode Global Config

no ip dhcp bootp automatic

This command disables the allocation of the addresses to the bootp client. The address are from the automatic address pool.

Format **no ip dhcp bootp automatic**
Mode Global Config

ip dhcp conflict logging

This command enables conflict logging on DHCP server.

Default	enabled
Format	**ip dhcp conflict logging**
Mode	Global Config

no ip dhcp conflict logging

This command disables conflict logging on DHCP server.

Format	**no ip dhcp conflict logging**
Mode	Global Config

clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database. If "*" is specified, the bindings corresponding to all the addresses are deleted. *<address>* is a valid IP address made up of four decimal bytes ranging from 0 to 255. IP address `0.0.0.0` is invalid.

Format	**clear ip dhcp binding** *{<address> | *}*
Mode	Privileged EXEC

clear ip dhcp server statistics

This command clears DHCP server statistics counters.

Format	**clear ip dhcp server statistics**
Mode	Privileged EXEC

clear ip dhcp conflict

The command is used to clear an address conflict from the DHCP Server database. The server detects conflicts using a ping. DHCP server clears all conflicts If the asterisk (*) character is used as the address parameter.

Default	none
Format	**clear ip dhcp conflict** *{<address> | *}*
Mode	Privileged EXEC

show ip dhcp binding

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Format	**show ip dhcp binding** *[<address>]*
Modes	• Privileged EXEC • User EXEC

Term	*Definition*
IP address	The IP address of the client.
Hardware Address	The MAC Address or the client identifier.
Lease expiration	The lease expiration time of the IP address assigned to the client.
Type	The manner in which IP address was assigned to the client.

show ip dhcp global configuration

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Format `show ip dhcp global configuration`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Service DHCP	The field to display the status of dhcp protocol.
Number of Ping Packets	The maximum number of Ping Packets that will be sent to verify that an ip address id not already assigned.
Conflict Logging	Shows whether conflict logging is enabled or disabled.
BootP Automatic	Shows whether BootP for dynamic pools is enabled or disabled.

show ip dhcp pool configuration

This command displays pool configuration. If **all** is specified, configuration for all the pools is displayed.

Format `show ip dhcp pool configuration {<name> | all}`

Modes
- Privileged EXEC
- User EXEC

Field	*Definition*
Pool Name	The name of the configured pool.
Pool Type	The pool type.
Lease Time	The lease expiration time of the IP address assigned to the client.
DNS Servers	The list of DNS servers available to the DHCP client .
Default Routers	The list of the default routers available to the DHCP client

The following additional field is displayed for Dynamic pool type:

Field	*Definition*
Network	The network number and the mask for the DHCP address pool.

The following additional fields are displayed for Manual pool type:

Field	*Definition*
Client Name	The name of a DHCP client.
Client Identifier	The unique identifier of a DHCP client.
Hardware Address	The hardware address of a DHCP client.
Hardware Address Type	The protocol of the hardware platform.
Host	The IP address and the mask for a manual binding to a DHCP client.

show ip dhcp server statistics

This command displays DHCP server statistics.

Format `show ip dhcp server statistics`

Modes
- Privileged EXEC
- User EXEC

Field	*Definition*
Automatic Bindings	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired Bindings	The number of expired leases.
Malformed Bindings	The number of truncated or corrupted messages that were received by the DHCP server.

Message Received:

Message	*Definition*
DHCP DISCOVER	The number of DHCPDISCOVER messages the server has received.
DHCP REQUEST	The number of DHCPREQUEST messages the server has received.
DHCP DECLINE	The number of DHCPDECLINE messages the server has received.
DHCP RELEASE	The number of DHCPRELEASE messages the server has received.
DHCP INFORM	The number of DHCPINFORM messages the server has received.

Message Sent:

Message	*Definition*
DHCP OFFER	The number of DHCPOFFER messages the server sent.
DHCP ACK	The number of DHCPACK messages the server sent.
DHCP NACK	The number of DHCPNACK messages the server sent.

show ip dhcp conflict

This command displays address conflicts logged by the DHCP Server. If no IP address is specified, all the conflicting addresses are displayed.

Format **show ip dhcp conflict** *[<ip-address>]*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
IP address	The IP address of the host as recorded on the DHCP server.
Detection Method	The manner in which the IP address of the hosts were found on the DHCP Server.
Detection time	The time when the conflict was found.

DNS CLIENT COMMANDS

These commands are used in the Domain Name System (DNS), an Internet directory service. DNS is how domain names are translated into IP addresses. When enabled, the DNS client provides a hostname lookup service to other components of Unified Switch.

ip domain lookup

Use this command to enable the DNS client.

Default enabled

Format **ip domain lookup**

Mode Global Config

no ip domain lookup

Use this command to disable the DNS client.

Format **no ip domain lookup**

Mode Global Config

ip domain name

Use this command to define a default domain name that Unified Switch software uses to complete unqualified host names (names with a domain name). By default, no default domain name is configured in the system. <*name*> may not be longer than 255 characters and should not include an initial period. This <*name*> should be used only when the default domain name list, configured using the **ip domain list command,** is empty.

Default none

Format **ip domain name** *<name>*

Mode Global Config

Example: The CLI command **ip domain name yahoo.com** will configure yahoo.com as a default domain name. For an unqualified hostname xxx, a DNS query is made to find the IP address corresponding to xxx.yahoo.com.

no ip domain name

Use this command to remove the default domain name configured using the **ip domain name** command.

Format	**no ip domain name**
Mode	Global Config

ip domain list

Use this command to define a list of default domain names to complete unqualified names. By default, the list is empty. Each name must be no more than 256 characters, and should not include an initial period. The default domain name, configured using the **ip domain name** command, is used only when the default domain name list is empty. A maximum of 32 names can be entered in to this list.

Default	none
Format	**ip domain list** *<name>*
Mode	Global Config

no ip domain list

Use this command to delete a name from a list.

Format	**no ip domain list** *<name>*
Mode	Global Config

ip name server

Use this command to configure the available name servers. Up to eight servers can be defined in one command or by using multiple commands. The parameter *<server-address>* is a valid IPv4 or IPv6 address of the server. The preference of the servers is determined by the order they were entered.

Format	**ip name-server <***server-address1***> [***server-address2...server-address8***]**
Mode	Global Config

no ip name server

Use this command to remove a name server.

Format	**no ip name-server [***server-address1...server-address8***]**
Mode	Global Config

ip host

Use this command to define static host name-to-address mapping in the host cache. <*name*> is host name. <i*p address*> is the IP address of the host.

Default	none
Format	**ip host** <*name*> <*ipaddress*>
Mode	Global Config

no ip host

Use this command to remove the name-to-address mapping.

Format	**no ip host** <*name*>
Mode	Global Config

ip domain retry

Use this command to specify the number of times to retry sending Domain Name System (DNS) queries. The parameter <*number*> indicates the number of times to retry sending a DNS query to the DNS server. This number ranges from 0 to 100.

Default	2
Format	**ip domain retry** <*number*>
Mode	Global Config

no ip domain retry

Use this command to return to the default.

Format	**no ip domain retry** <*number*>
Mode	Global Config

ip domain timeout

Use this command to specify the amount of time to wait for a response to a DNS query. The parameter <*seconds*> specifies the time, in seconds, to wait for a response to a DNS query. <*seconds*> ranges from 0 to 3600.

Default	3
Format	**ip domain timeout** <*seconds*>
Mode	Global Config

no ip domain timeout

Use this command to return to the default setting.

Format	**no ip domain timeout** <*seconds*>
Mode	Global Config

clear host

Use this command to delete entries from the host name-to-address cache. This command clears the entries from the DNS cache maintained by the software. This command clears both IPv4 and IPv6 entries.

Format `clear host {<name> | all}`

Mode Privileged EXEC

Field	*Description*
name	A particular host entry to remove. <*name*> ranges from 1-255 characters.
all	Removes all entries.

show hosts

Use this command to display the default domain name, a list of name server hosts, the static and the cached list of host names and addresses. <*name*> ranges from 1-255 characters. This command displays both IPv4 and IPv6 entries.

Format `show hosts [name]`

Mode User EXEC

Field	*Description*
Host Name	Domain host name.
Default Domain	Default domain name.
Default Domain List	Default domain list.
Domain Name Lookup	DNS client enabled/disabled.
Number of Retries	Number of time to retry sending Domain Name System (DNS) queries.
Retry Timeout Period	Amount of time to wait for a response to a DNS query.
Name Servers	Configured name servers.

Example: The following shows example CLI display output for the command.

```
<DWS-4026> show hosts

Host name..................... Device
Default domain................ gm.com
Default domain list........... yahoo.com, Stanford.edu, rediff.com
Domain Name lookup............ Enabled
Number of retries............. 5
Retry timeout period.......... 1500
Name servers (Preference order)... 176.16.1.18 176.16.1.19


Configured host name-to-address mapping:

Host                          Addresses
```

```
------------------------------ ------------------------------
accounting.gm.com              176.16.8.8

Host              Total     Elapsed   Type      Addresses
---------------   -------   -------   --------  --------------
www.stanford.edu   72    3            IP        171.64.14.203
```

SERVICEABILITY PACKET TRACING COMMANDS

These commands improve the capability of network engineers to diagnose conditions affecting their Unified Switch product.

Caution! The output of “debug” commands can be long and may adversely affect system performance.

debug arp

Use this command to enable ARP debug protocol messages.

Default	disabled
Format	**`debug arp`**
Mode	Privileged EXEC

no debug arp

Use this command to disable ARP debug protocol messages.

Format	**`no debug arp`**
Mode	Privileged EXEC

debug auto-voip

Use this command to enable Auto VOIP debug messages. Use the optional parameters to trace H323, SCCP, or SIP packets respectively.

Default	disabled
Format	**`debug auto-voip [H323|SCCP|SIP]`**
Mode	Privileged EXEC

no debug auto-voip

Use this command to disable Auto VOIP debug messages.

Format	**`no debug auto-voip`**
Mode	Privileged EXEC

debug clear

This command disables all previously enabled “debug” traces.

Default	disabled
Format	`debug clear`
Mode	Privileged EXEC

debug console

This command enables the display of “debug” trace output on the login session in which it is executed. Debug console display must be enabled in order to view any trace output. The output of debug trace commands will appear on all login sessions for which debug console has been enabled. The configuration of this command remains in effect for the life of the login session. The effect of this command is not persistent across resets.

Default	disabled
Format	`debug console`
Mode	Privileged EXEC

no debug console

This command disables the display of “debug” trace output on the login session in which it is executed.

Format	`no debug console`
Mode	Privileged EXEC

debug dot1x packet

Use this command to enable dot1x packet debug trace.

Default	disabled
Format	`debug dot1x`
Mode	Privileged EXEC

no debug dot1x packet

Use this command to disable dot1x packet debug trace.

Format	`no debug dot1x`
Mode	Privileged EXEC

debug igmpsnooping packet

This command enables tracing of IGMP Snooping packets received and transmitted by the switch.

Default	disabled
Format	`debug igmpsnooping packet`
Mode	Privileged EXEC

no debug igmpsnooping packet

This command disables tracing of IGMP Snooping packets.

Format	`no debug igmpsnooping packet`
Mode	Privileged EXEC

debug igmpsnooping packet transmit

This command enables tracing of IGMP Snooping packets transmitted by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default	disabled
Format	`debug igmpsnooping packet transmit`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]: igmp_snooping_debug.c(116) 908 %
Pkt TX - Intf: 0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:00 Dest_Mac: 01:00:5e:00:00:01
Src_IP: 9.1.1.1 Dest_IP: 225.0.0.1 Type: V2_Membership_Report Group: 225.0.0.1
```

The following parameters are displayed in the trace message:

Parameter	*Definition*
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is slot/port (internal interface number).
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the IP header in the packet.
Dest_IP	The destination multicast IP address in the packet.
Type	The type of IGMP packet. Type can be one of the following: • `Membership Query` – IGMP Membership Query • `V1_Membership_Report` – IGMP Version 1 Membership Report • `V2_Membership_Report` – IGMP Version 2 Membership Report • `V3_Membership_Report` – IGMP Version 3 Membership Report • `V2_Leave_Group` – IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

no debug igmpsnooping transmit

This command disables tracing of transmitted IGMP snooping packets.

Format	`no debug igmpsnooping transmit`
Mode	Privileged EXEC

debug igmpsnooping packet receive

This command enables tracing of IGMP Snooping packets received by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default	disabled
Format	**debug igmpsnooping packet receive**
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]: igmp_snooping_debug.c(116) 908 %
Pkt RX - Intf: 0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:10 Dest_Mac: 01:00:5e:00:00:05
Src_IP: 11.1.1.1 Dest_IP: 225.0.0.5 Type: Membership_Query Group: 225.0.0.5
```

The following parameters are displayed in the trace message:

Parameter	*Definition*
RX	A packet received by the device.
Intf	The interface that the packet went out on. Format used is slot/port (internal interface number).
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the ip header in the packet.
Dest_IP	The destination multicast ip address in the packet.
Type	The type of IGMP packet. Type can be one of the following: • `Membership_Query` – IGMP Membership Query • `V1_Membership_Report` – IGMP Version 1 Membership Report • `V2_Membership_Report` – IGMP Version 2 Membership Report • `V3_Membership_Report` – IGMP Version 3 Membership Report • `V2_Leave_Group` – IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

no debug igmpsnooping receive

This command disables tracing of received IGMP Snooping packets.

Format	**no debug igmpsnooping receive**
Mode	Privileged EXEC

debug ip acl

Use this command to enable debug of IP Protocol packets matching the ACL criteria.

Default	disabled
Format	**debug ip acl** *<acl Number>*
Mode	Privileged EXEC

no debug ip acl

Use this command to disable debug of IP Protocol packets matching the ACL criteria.

Format	**no debug ip acl <acl Number>**
Mode	Privileged EXEC

debug ip vrrp

Use this command to enable VRRP debug protocol messages.

Default	disabled
Format	**debug ip vrrp**
Mode	Privileged EXEC

no debug ip vrrp

Use this command to disable VRRP debug protocol messages.

Format	**no debug ip vrrp**
Mode	Privileged EXEC

debug lacp packet

This command enables tracing of LACP packets received and transmitted by the switch.

Default	disabled
Format	**debug lacp packet**
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 14:04:51 10.254.24.31-1 DOT3AD[183697744]: dot3ad_debug.c(385) 58 %%
 Pkt TX - Intf: 0/1(1), Type: LACP, Sys: 00:11:88:14:62:e1, State: 0x47, Key:
0x36
```

no debug lacp packet

This command disables tracing of LACP packets.

Format	**no debug lacp packet**
Mode	Privileged EXEC

debug mldsnooping packet

Use this command to trace MLD snooping packet reception and transmission. **receive** traces only received MLD snooping packets and **transmit** traces only transmitted MLD snooping packets. When neither keyword is used in the command, then all MLD snooping packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default	disabled
Format	**debug mldsnooping packet [receive|transmit]**
Mode	Privileged EXEC

no debug mldsnooping packet

Use this command to disable debug tracing of MLD snooping packet reception and transmission.

debug ping packet

This command enables tracing of ICMP echo requests and responses. The command traces pings on the network port/serviceport for switching packages. For routing packages, pings are traced on the routing ports as well.

Default	disabled
Format	**debug ping packet**
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 00:21:22 192.168.17.29-1 SIM[181040176]: sim_debug.c(128) 20 % Pkt TX - Intf:
0/1(1),
SRC_IP:10.50.50.2, DEST_IP:10.50.50.1, Type:ECHO_REQUEST


<15> JAN 01 00:21:22 192.168.17.29-1 SIM[182813968]: sim_debug.c(82) 21 % Pkt RX - Intf: 0/
1(1), S
RC_IP:10.50.50.1, DEST_IP:10.50.50.2, Type:ECHO_REPLY
```

The following parameters are displayed in the trace message:

Parameter	*Definition*
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on. Format used is slot/port (internal interface number).
SRC_IP	The source IP address in the IP header in the packet.
DEST_IP	The destination IP address in the IP header in the packet.
Type	Type determines whether or not the ICMP message is a REQUEST or a RESPONSE.

no debug ping packet

This command disables tracing of ICMP echo requests and responses.

Format	**no debug ping packet**
Mode	Privileged EXEC

debug rip packet

This command turns on tracing of RIP requests and responses. This command takes no options. The output is directed to the log file.

Default	disabled
Format	`debug rip packet`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 00:35:15 192.168.17.29-1 RIP[181783160]: rip_map_debug.c(96) 775 %
Pkt RX on Intf: 0/1(1), Src_IP:43.1.1.1 Dest_IP:43.1.1.2
Rip_Version: RIPv2 Packet_Type:RIP_RESPONSE
ROUTE 1): Network: 10.1.1.0 Mask: 255.255.255.0 Metric: 1
ROUTE 2): Network: 40.1.0.0 Mask: 255.255.0.0 Metric: 1
ROUTE 3): Network: 10.50.50.0 Mask: 255.255.255.0 Metric: 1
ROUTE 4): Network: 41.1.0.0 Mask: 255.255.0.0 Metric: 1
ROUTE 5): Network:42.0.0.0 Mask:255.0.0.0 Metric:1
Another 6 routes present in packet not displayed.
```

The following parameters are displayed in the trace message:

Parameter	*Definition*
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on. Format used is slot/port (internal interface number).
Src_IP	The source IP address in the IP header of the packet.
Dest_IP	The destination IP address in the IP header of the packet.
Rip_Version	RIP version used <RIPv1 or RIPv2>.
Packet_Type	Type of RIP packet. <RIP_REQUEST or RIP_RESPONSE>.
Routes	Up to 5 routes in the packet are displayed in the following format: `Network: <a.b.c.d> Mask <a.b.c.d> Next_Hop <a.b.c.d> Metric <a>` The next hop is only displayed if it is different from `0.0.0.0`. For RIPv1 packets, Mask is always `0.0.0.0`.
Number of routes not printed	Only the first five routes present in the packet are included in the trace. There is another notification of the number of additional routes present in the packet that were not included in the trace.

no debug rip packet

This command disables tracing of RIP requests and responses.

Format	`no debug rip packet`
Mode	Privileged EXEC

debug sflow packet

Use this command to enable sFlow debug packet trace.

Default disabled
Format `debug sflow packet`
Mode Privileged EXEC

no debug sflow packet

Use this command to disable sFlow debug packet trace.

Format `no debug sflow packet`
Mode Privileged EXEC

debug spanning-tree bpdu

This command enables tracing of spanning tree BPDUs received and transmitted by the switch.

Default disabled
Format `debug spanning-tree bpdu`
Mode Privileged EXEC

no debug spanning-tree bpdu

This command disables tracing of spanning tree BPDUs.

Format `no debug spanning-tree bpdu`
Mode Privileged EXEC

debug spanning-tree bpdu receive

This command enables tracing of spanning tree BPDUs received by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets for a particular interface.

Default disabled
Format `debug spanning-tree bpdu receive`
Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt RX -
Intf: 0/9(9), Source_Mac: 00:11:88:4e:c2:10 Version: 3, Root Mac: 00:11:88:4e:c2:00, Root
Priority: 0x8000 Path Cost: 0
```

The following parameters are displayed in the trace message:

Parameter	*Definition*
RX	A packet received by the device.
Intf	The interface that the packet came in on. Format used is unit/port/slot (internal interface number). Unit is always shown as 1.

Parameter	*Definition*
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

no debug spanning-tree bpdu receive

This command disables tracing of received spanning tree BPDUs.

Format `no debug spanning-tree bpdu receive`

Mode Privileged EXEC

debug spanning-tree bpdu transmit

This command enables tracing of spanning tree BPDUs transmitted by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets on a particular interface.

Default disabled

Format `debug spanning-tree bpdu transmit`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt TX -
Intf: 0/7(7), Source_Mac: 00:11:88:4e:c2:00 Version: 3, Root_Mac: 00:11:88:4e:c2:00,
Root_Priority: 0x8000 Path_Cost: 0
```

The following parameters are displayed in the trace message:

Parameter	*Definition*
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is unit/port/slot (internal interface number). Unit is always shown as 1.
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

no debug spanning-tree bpdu transmit

This command disables tracing of transmitted spanning tree BPDUs.

Format	**`no debug spanning-tree bpdu transmit`**
Mode	Privileged EXEC

logging persistent

Use this command to configure the Persistent logging for the switch. The severity level of logging messages is specified at severity level. Possible values for severity level are *`(emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7)`*.

Default	Disable
Format	**`logging persistent`** *`<severity level>`*
Mode	Global Config

no logging persistent

Use this command to disable the persistent logging in the switch.

Format	**`no logging persistent`**
Mode	Global Config

CABLE TEST COMMAND

The cable test feature enables you to determine the cable connection status on a selected port.

Note: The cable test feature is supported only for copper cable. It is not supported for optical fiber cable.

If the port has an active link while the cable test is run, the link can go down for the duration of the test.

cablestatus

This command returns the status of the specified port.

Format	**cablestatus** *<slot/port>*
Mode	Privileged EXEC

Field	*Description*
Cable Status	One of the following statuses is returned: • **Normal**: The cable is working correctly. • **Open**: The cable is disconnected or there is a faulty connector. • **Short**: There is an electrical short in the cable. • **Cable Test Failed**: The cable status could not be determined. The cable may in fact be working.
Cable Length	If this feature is supported by the PHY for the current link speed, the cable length is displayed as a range between the shortest estimated length and the longest estimated length. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status may display as Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded. Unknown is displayed if the cable length could not be determined.

sFLOW COMMANDS

sFlow® is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

sflow receiver

Use this command to configure the sFlow collector parameters (owner string, receiver timeout, max datagram size, IP address, and port).

Format `sflow receiver <rcvr_idx> owner <owner-string> timeout <rcvr_timeout> max datagram <size> ip/ipv6 <ip> port <port>`

Mode Global Config

Field	*Description*
Receiver Owner	The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. The default is a null string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.
Receiver Timeout	The time, in seconds, remaining before the sampler or poller is released and stops sending samples to receiver. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. The allowed range is 0-4294967295 seconds. The default is zero (0).
Receiver Max Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. The management entity should set this value to avoid fragmentation of the sFlow datagrams. The allowed range is 200 to 9116). The default is 1400.
Receiver IP	The sFlow receiver IP address. If set to 0.0.0.0, no sFlow datagrams will be sent. The default is 0.0.0.0.
Receiver Port	The destination Layer4 UDP port for sFlow datagrams. The range is 1-65535. The default is 6343.

no sflow receiver

Use this command to set the sFlow collector parameters back to the defaults.

Format `no sflow receiver <indx> {ip <ip-address> | maxdatagram <size> | owner <string> timeout <interval> | port <14-port>}`

Mode Global Config

sflow sampler

A data source configured to collect flow samples is called a sampler. Use this command to configure a new sFlow sampler instance for this data source if <*rcvr_idx*> is valid.

Format `sflow sampler {<rcvr-indx> | rate <sampling-rate> | maxheadersize <size>}`

Mode Interface Config

Field	*Description*
Receiver Index	The sFlow Receiver for this sFlow sampler to which flow samples are to be sent. A value of zero (0) means that no receiver is configured, no packets will be sampled. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. Possible values are 1-8. The default is 0.
Maxheadersize	The maximum number of bytes that should be copied from the sampler packet. The range is 20-256. The default is 128. When set to zero (0), all the sampler parameters are set to their corresponding default value.
Sampling Rate	The statistical sampling rate for packet sampling from this source. A sampling rate of 1 counts all packets. A value of zero (0) disables sampling. A value of N means that out of N incoming packets, 1 packet will be sampled. The range is 1024-65536 and 0. The default is 0.

no sflow sampler

Use this command to reset the sFlow sampler instance to the default settings.

Format `no sflow sampler {<rcvr-indx> | rate <sampling-rate> | maxheadersize <size>}`

Mode Interface Config

sflow poller

A data source configured to collect counter samples is called a poller. Use this command to enable a new sFlow poller instance for this data source if <*rcvr_idx*> is valid.

Format `sflow poller {<rcvr-indx> | interval <poll-interval>}`

Mode Interface Config

Field	*Description*
Receiver Index	Enter the sFlow Receiver associated with the sampler/poller. A value of zero (0) means that no receiver is configured. The range is 1-8. The default is 0.
Poll Interval	Enter the sFlow instance polling interval. A poll interval of zero (0) disables counter sampling. When set to zero (0), all the poller parameters are set to their corresponding default value. The range is 0-86400. The default is 0. A value of N means once in N seconds a counter sample is generated.

no sflow poller

Use this command to reset the sFlow poller instance to the default settings.

Format `no sflow poller {<rcvr-indx> | interval <poll-interval>}`

Mode Interface Config

show sflow agent

The sFlow agent collects time-based sampling of network interface statistics and flow-based samples. These are sent to the configured sFlow receivers. Use this command to display the sFlow agent information.

Format `show sflow agent`

Mode Privileged EXEC

Field	*Description*
sFlow Version	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version; Organization; Software Revision where: • MIB Version: 1.3, the version of this MIB. • Organization: D-Link Corporation. • Revision: D-Link UWS Software version
IP Address	The IP address associated with this agent.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show sflow agent

sFlow Version..................................... 1.3;D-Link Corporation;1.0
IP Address........................................ 10.131.12.66
```

show sflow pollers

Use this command to display the sFlow polling instances created on the switch. Use "-" for range.

Format `show sflow pollers`

Mode Privileged EXEC

Field	*Description*
Poller Data Source	The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.
Receiver Index	The sFlowReceiver associated with this sFlow counter poller.
Poller Interval	The number of seconds between successive samples of the counters associated with this data source.

show sflow receivers

Use this command to display configuration information related to the sFlow receivers.

Format `show sflow receivers [<index>]`

Mode Privileged EXEC

Field	*Description*
Receiver Index	The sFlow Receiver associated with the sampler/poller.
Owner String	The identity string for receiver, the entity making use of this sFlowRcvrTable entry.
Time Out	The time (in seconds) remaining before the receiver is released and stops sending samples to sFlow receiver.
Max Datagram Size	The maximum number of bytes that can be sent in a single sFlow datagram.
Port	The destination Layer4 UDP port for sFlow datagrams.

Field	*Description*
IP Address	The sFlow receiver IP address.
Address Type	The sFlow receiver IP address type. For an IPv4 address, the value is 1 and for an IPv6 address, the value is 2.
Datagram Version	The sFlow protocol version to be used while sending samples to sFlow receiver.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show sflow receivers 1
Receiver Index.............................. 1
Owner String................................
Time out.................................... 0
IP Address:................................. 0.0.0.0
Address Type................................ 1
Port........................................ 6343
Datagram Version............................ 5
Maximum Datagram Size....................... 1400
```

show sflow samplers

Use this command to display the sFlow sampling instances created on the switch.

Format `show sflow samplers`

Mode Privileged EXEC

Field	*Description*
Sampler Data Source	The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.
Receiver Index	The sFlowReceiver configured for this sFlow sampler.
Packet Sampling Rate	The statistical sampling rate for packet sampling from this source.
Max Header Size	The maximum number of bytes that should be copied from a sampled packet to form a flow sample.

AUTOINSTALL COMMANDS

The AutoInstall feature enables the automatic configuration of a switch when the device is initialized and no configuration file is found on the switch. When no configuration file is found, it is downloaded from a TFTP server and saved to non-volatile memory. The TFTP server name or address is provided by a DHCP server in response to a IP address request initiated during startup.

boot autoinstall

The command enables/disables autoinstall on the switch.

Default	`enable`
Format	`boot autoinstall {start | stop}`
Mode	Privileged EXEC

boot autoinstall auto-save

This command enables or disables saving the network configuration to non-volatile memory. When enabled, the configuration is saved after downloading from the TFTP server without operator intervention. When disabled, the operator must explicitly save the configuration, if needed.

Default	`enable`
Format	`boot autoinstall auto-save`
Mode	Privileged EXEC

no boot autoinstall auto-save

This command disables saving the network configuration to non-volatile memory.

boot autoinstall retry-count

This command sets the number of unicast TFTP attempts for the configuration file.

Default	`3`
Format	**`boot autoinstall retry-count <1-6>`**
Mode	Privileged EXEC

no boot autoinstall retry-count

This command sets to the default the number of unicast TFTP attempts for the configuration file.

Format	**`no boot autoinstall retry-count`**
Mode	Privileged EXEC

show autoinstall

This command displays the current status of the AutoInstall process.

Format	**show autoinstall**
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show autoinstall

AutoInstall Mode.............................. Started
AutoSave Mode................................. Enabled
AutoInstall Retry Count....................... 3
AutoInstall State............................. Waiting for boot options
```


Section 9: Management Commands

This section describes the management commands available in the Unified Switch CLI.

The Management Commands section contains the following subsections:

Note: The commands in this section are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

Network Interface Commands

This section describes the commands you use to configure a logical interface for management access. To configure the management VLAN, see "network mgmt_vlan" on page 32.

enable (Privileged EXEC access)

This command gives you access to the Privileged EXEC mode. From the Privileged EXEC mode, you can configure the network interface.

Format	`enable`
Mode	User EXEC

network parms

This command sets the IP address, subnet mask and gateway of the device. The IP address and the gateway must be on the same subnet.

Format	**network parms** *<ipaddr> <netmask> [<gateway>]*
Mode	Privileged EXEC

network protocol

This command specifies the network configuration protocol to be used. If you modify this value, change is effective immediately. If you use the *bootp* parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the *dhcp* parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the *none* parameter, you must configure the network information for the switch manually.

Default	none
Format	**network protocol** *{none | bootp | dhcp}*
Mode	Privileged EXEC

network mac-address

This command sets locally administered MAC addresses. The following rules apply:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (b'0') or locally administered (b'1').
- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (b'0') or a group address (b'1').
- The second character, of the twelve character macaddr, must be 2, 6, A or E.

A locally administered address must have bit 6 On (b'1') and bit 7 Off (b'0').

Format	**network mac-address** *<macaddr>*
Mode	Privileged EXEC

network mac-type

This command specifies whether the switch uses the burned in MAC address or the locally-administered MAC address.

Default	burnedin
Format	**network mac-type** *{local | burnedin}*
Mode	Privileged EXEC

no network mac-type

This command resets the value of MAC address to its default.

Format	**no network mac-type**
Mode	Privileged EXEC

network javamode

This command specifies whether or not the switch should allow access to the Java applet in the header frame of the Web interface and to the WLAN Visualization applet. When access is enabled, the Java applets can be viewed from the Web interface. When access is disabled, the user cannot view the Java applets.

Default enabled

Format `network javamode`

Mode Privileged EXEC

no network javamode

This command disallows access to the Java applet in the header frame of the Web interface. When access is disabled, the user cannot view the Java applet.

Format `no network javamode`

Mode Privileged EXEC

show network

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed. The network interface is always considered to be up, whether or not any member ports are up; therefore, the show network command will always show “Interface Status” as “Up”.

Format `show network`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface Status	The network interface status; it is always considered to be “up”.
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
Burned In MAC Address	The burned in MAC address used for in-band connectivity.
Locally Administered MAC Address	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique BridgeIdentifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	The MAC address which should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.

Term	*Definition*
Network Configuration Protocol Current	The network protocol being used. The options are bootp | dhcp | none.

Example: The following shows example CLI display output for the network port.

```
(admin) #show network

Interface Status.............................. Always Up
IP Address.................................... 10.250.3.1
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 10.250.3.3
Burned In MAC Address......................... 00:10:18:82:03:37
Locally Administered MAC Address.............. 00:00:00:00:00:00
MAC Address Type.............................. Burned In
Network Configuration Protocol Current........ None
Management VLAN ID............................ 1
```

CONSOLE PORT ACCESS COMMANDS

This section describes the commands you use to configure the console port. You can use a serial cable to connect a management host directly to the console port of the switch.

configuration

This command gives you access to the Global Config mode. From the Global Config mode, you can configure a variety of system settings, including user accounts. From the Global Config mode, you can enter other command modes, including Line Config mode.

Format	**`configuration`**
Mode	Privileged EXEC

lineconfig

This command gives you access to the Line Config mode, which allows you to configure various Telnet settings and the console port.

Format	**`lineconfig`**
Mode	Global Config

serial baudrate

This command specifies the communication rate of the terminal interface. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Default	9600
Format	**`serial baudrate`** *{1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}*
Mode	Line Config

no serial baudrate

This command sets the communication rate of the terminal interface.

Format `no serial baudrate`

Mode Line Config

serial timeout

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

Default 5

Format `serial timeout <0-160>`

Mode Line Config

no serial timeout

This command sets the maximum connect time (in minutes) without console activity.

Format `no serial timeout`

Mode Line Config

show serial

This command displays serial communication settings for the switch.

Format `show serial`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Serial Port Login Timeout (minutes)	The time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.
Baud Rate (bps)	The default baud rate at which the serial port will try to connect. The available values are 1200, 2400, 4800, 9600, 19200, 38400,57600, and 115200 baud. The factory default is 9600 baud.
Character Size (bits)	The number of bits in a character. The number of bits is always 8.
Flow Control	Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.
Stop Bits	The number of Stop bits per character. The number of Stop bits is always 1.
Parity Type	The Parity Method used on the Serial Port. The Parity Method is always None.

TELNET COMMANDS

This section describes the commands you use to configure and view Telnet settings. You can use Telnet to manage the device from a remote management host.

ip telnet server enable

Use this command to enable Telnet connections to the system and to enable the Telnet Server Admin Mode. This command opens the Telnet listening port.

Default	enabled
Format	**`ip telnet server enable`**
Mode	Privileged EXEC

no ip telnet server enable

Use this command to disable Telnet access to the system and to disable the Telnet Server Admin Mode. This command closes the Telnet listening port and disconnects all open Telnet sessions.

Format	**`no ip telnet server enable`**
Mode	Privileged EXEC

telnet

This command establishes a new outbound Telnet connection to a remote host. The *host* value must be a valid IP address or host name. Valid values for *port* should be a valid decimal integer in the range of 0 to 65535, where the default value is 23. If *`[debug]`* is used, the current Telnet options enabled is displayed. The optional *line* parameter sets the outbound Telnet operational mode as linemode where, by default, the operational mode is character mode. The *noecho* option disables local echo.

Format	**`telnet`** *`<ip-address|hostname> <port> [debug] [line] [noecho]`*
Modes	• Privileged EXEC • User EXEC

transport input telnet

This command regulates new Telnet sessions. If enabled, new Telnet sessions can be established until there are no more sessions available. An established session remains active until the session is ended or an abnormal network error ends the session.

Note: If the Telnet Server Admin Mode is disabled, Telnet sessions cannot be established. Use the **`ip telnet server enable`** command to enable Telnet Server Admin Mode.

Default	enabled
Format	**`transport input telnet`**
Mode	Line Config

no transport input telnet

Use this command to prevent new Telnet sessions from being established.

Format	**`no transport input telnet`**
Mode	Line Config

transport output telnet

This command regulates new outbound Telnet connections. If enabled, new outbound Telnet sessions can be established until the system reaches the maximum number of simultaneous outbound Telnet sessions allowed. An established session remains active until the session is ended or an abnormal network error ends it.

Default	enabled
Format	**`transport output telnet`**
Mode	Line Config

no transport output telnet

Use this command to prevent new outbound Telnet connection from being established.

Format	**`no transport output telnet`**
Mode	Line Config

session-limit

This command specifies the maximum number of simultaneous outbound Telnet sessions. A value of 0 indicates that no outbound Telnet session can be established.

Default	5
Format	**`session-limit`** *`<0-5>`*
Mode	Line Config

no session-limit

This command sets the maximum number of simultaneous outbound Telnet sessions to the default value.

Format	**`no session-limit`**
Mode	Line Config

session-timeout

This command sets the Telnet session timeout value.The timeout value unit of time is minutes.

Default	5
Format	**`session-timeout`** *`<1-160>`*
Mode	Line Config

no session-timeout

This command sets the Telnet session timeout value to the default. The timeout value unit of time is minutes.

Format	**no session-timeout**
Mode	Line Config

telnetcon maxsessions

This command specifies the maximum number of Telnet connection sessions that can be established. A value of 0 indicates that no Telnet connection can be established. The range is 0-5.

Default	5
Format	**telnetcon maxsessions** *<0-5>*
Mode	Privileged EXEC

no telnetcon maxsessions

This command sets the maximum number of Telnet connection sessions that can be established to the default value.

Format	**no telnetcon maxsessions**
Mode	Privileged EXEC

telnetcon timeout

This command sets the Telnet connection session timeout value, in minutes. A session is active as long as the session has not been idle for the value set. The time is a decimal value from 1 to 160.

Note: When you change the timeout value, the new value is applied to all active and inactive sessions immediately. Any sessions that have been idle longer than the new timeout value are disconnected immediately.

Default	5
Format	**telnetcon timeout** *<1-160>*
Mode	Privileged EXEC

no telnetcon timeout

This command sets the Telnet connection session timeout value to the default.

Note: Changing the timeout value for active sessions does not become effective until the session is reaccessed. Also, any keystroke activates the new timeout duration.

Format	**no telnetcon timeout**
Mode	Privileged EXEC

show telnet

This command displays the current outbound Telnet settings. In other words, these settings apply to Telnet connections initiated from the switch to a remote system.

Format `show telnet`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Outbound Telnet Login Timeout	The number of minutes an outbound Telnet session is allowed to remain inactive before being logged off.
Maximum Number of Outbound Telnet Sessions	The number of simultaneous outbound Telnet connections allowed.
Allow New Outbound Telnet Sessions	Indicates whether outbound Telnet sessions will be allowed.

show telnetcon

This command displays the current inbound Telnet settings. In other words, these settings apply to Telnet connections initiated from a remote system to the switch.

Format `show telnetcon`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Remote Connection Login Timeout (minutes)	This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from 1 to 160. The factory default is 5.
Maximum Number of Remote Connection Sessions	This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.
Allow New Telnet Sessions	New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.

SECURE SHELL COMMANDS

This section describes the commands you use to configure Secure Shell (SSH) access to the switch. Use SSH to access the switch from a remote management host.

Note: The system allows a maximum of 5 SSH sessions.

ip ssh

Use this command to enable SSH access to the system. (This command is the short form of the **ip ssh server enable** command.)

Default	disabled
Format	**ip ssh**
Mode	Privileged EXEC

ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

Default	1 and 2
Format	**ip ssh protocol** *[1] [2]*
Mode	Privileged EXEC

ip ssh server enable

This command enables the IP secure shell server.

Default	disabled
Format	**ip ssh server enable**
Mode	Privileged EXEC

no ip ssh server enable

This command disables the IP secure shell server.

Format	**no ip ssh server enable**
Mode	Privileged EXEC

sshcon maxsessions

This command specifies the maximum number of SSH connection sessions that can be established. A value of 0 indicates that no ssh connection can be established. The range is 0 to 5.

Default	5
Format	**sshcon maxsessions** *<0-5>*
Mode	Privileged EXEC

no sshcon maxsessions

This command sets the maximum number of allowed SSH connection sessions to the default value.

Format	**no sshcon maxsessions**
Mode	Privileged EXEC

sshcon timeout

This command sets the SSH connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. The time is a decimal value from 1 to 160.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

Default	5
Format	**sshcon timeout** *<1-160>*
Mode	Privileged EXEC

no sshcon timeout

This command sets the SSH connection session timeout value, in minutes, to the default.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

Format	**no sshcon timeout**
Mode	Privileged EXEC

show ip ssh

This command displays the ssh settings.

Format	**show ip ssh**
Mode	Privileged EXEC

Term	*Definition*
Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
Protocol Level	The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.
SSH Sessions Currently Active	The number of SSH sessions currently active.
Max SSH Sessions Allowed	The maximum number of SSH sessions allowed.
SSH Timeout	The SSH timeout value in minutes.
Keys Present	Indicates whether the SSH RSA and DSA key files are present on the device.
Key Generation in Progress	Indicates whether RSA or DSA key files generation is currently in progress.

MANAGEMENT SECURITY COMMANDS

This section describes commands you use to generate keys and certificates, which you can do in addition to loading them as before.

crypto certificate generate

Use this command to generate self-signed certificate for HTTPS. The generate RSA key for SSL has a length of 1024 bits. The resulting certificate is generated with a common name equal to the lowest IP address of the device and a duration of 365 days.

Format	`crypto certificate generate`
Mode	Global Config

no crypto certificate generate

Use this command to delete the HTTPS certificate files from the device, regardless of whether they are self-signed or downloaded from an outside source.

Format	`no crypto certificate generate`
Mode	Global Config

crypto key generate rsa

Use this command to generate an RSA key pair for SSH. The new key files will overwrite any existing generated or downloaded RSA key files.

Format	`crypto key generate rsa`
Mode	Global Config

no crypto key generate rsa

Use this command to delete the RSA key files from the device.

Format	`no crypto key generate rsa`
Mode	Global Config

crypto key generate dsa

Use this command to generate a DSA key pair for SSH. The new key files will overwrite any existing generated or downloaded DSA key files.

Format	`crypto key generate dsa`
Mode	Global Config

no crypto key generate dsa

Use this command to delete the DSA key files from the device.

Format	`no crypto key generate dsa`
Mode	Global Config

HYPERTEXT TRANSFER PROTOCOL COMMANDS

This section describes the commands you use to configure Hypertext Transfer Protocol (HTTP) and secure HTTP access to the switch. Access to the switch by using a Web browser is enabled by default. Everything you can view and configure by using the CLI is also available by using the Web.

ip http server

This command enables access to the switch through the Web interface. When access is enabled, the user can login to the switch from the Web interface. When access is disabled, the user cannot login to the switch's Web server. Disabling the Web interface takes effect immediately. All interfaces are affected.

Default	enabled
Format	`ip http server`
Mode	Privileged EXEC

no ip http server

This command disables access to the switch through the Web interface. When access is disabled, the user cannot login to the switch's Web server.

Format	`no ip http server`
Mode	Privileged EXEC

ip http secure-server

This command is used to enable the secure socket layer for secure HTTP.

Default	disabled
Format	`ip http secure-server`
Mode	Privileged EXEC

no ip http secure-server

This command is used to disable the secure socket layer for secure HTTP.

Format	`no ip http secure-server`
Mode	Privileged EXEC

ip http java

This command enables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

Default	Enabled
Format	`ip http java`
Mode	Privileged EXEC

no ip http java

This command disables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

Format **no ip http java**
Mode Privileged EXEC

ip http session hard-timeout

This command configures the hard timeout for un-secure HTTP sessions in hours. Configuring this value to zero will give an infinite hard-timeout. When this timeout expires, the user will be forced to re-authenticate. This timer begins on initiation of the web session and is unaffected by the activity level of the connection.

Default 24
Format **ip http session hard-timeout** *<0-168>*
Mode Privileged EXEC

no ip http session hard-timeout

This command restores the hard timeout for un-secure HTTP sessions to the default value.

Format **no ip http session hard-timeout**
Mode Privileged EXEC

ip http session maxsessions

This command limits the number of allowable un-secure HTTP sessions. Zero is the configurable minimum.

Default 16
Format **ip http session maxsessions** *<0-16>*
Mode Privileged EXEC

no ip http session maxsessions

This command restores the number of allowable un-secure HTTP sessions to the default value.

Format **no ip http session maxsessions**
Mode Privileged EXEC

ip http session soft-timeout

This command configures the soft timeout for un-secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires the user will be forced to re-authenticate. This timer begins on initiation of the Web session and is re-started with each access to the switch.

Default 5
Format **ip http session soft-timeout** *<0-60>*
Mode Privileged EXEC

no ip http session soft-timeout

This command resets the soft timeout for un-secure HTTP sessions to the default value.

Format **no ip http session soft-timeout**
Mode Privileged EXEC

ip http secure-session hard-timeout

This command configures the hard timeout for secure HTTP sessions in hours. When this timeout expires, the user is forced to re-authenticate. This timer begins on initiation of the Web session and is unaffected by the activity level of the connection. The secure-session hard-timeout can not be set to zero (infinite).

Default 24
Format **ip http secure-session hard-timeout** *<1-168>*
Mode Privileged EXEC

no ip http secure-session hard-timeout

This command resets the hard timeout for secure HTTP sessions to the default value.

Format **no ip http secure-session hard-timeout**
Mode Privileged EXEC

ip http secure-session maxsessions

This command limits the number of secure HTTP sessions. Zero is the configurable minimum.

Default 16
Format **ip http secure-session maxsessions** *<0-16>*
Mode Privileged EXEC

no ip http secure-session maxsessions

This command restores the number of allowable secure HTTP sessions to the default value.

Format **no ip http secure-session maxsessions**
Mode Privileged EXEC

ip http secure-session soft-timeout

This command configures the soft timeout for secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires, you are forced to re-authenticate. This timer begins on initiation of the Web session and is re-started with each access to the switch. The secure-session soft-timeout can not be set to zero (infinite).

Default 5
Format **ip http secure-session soft-timeout** *<1-60>*
Mode Privileged EXEC

no ip http secure-session soft-timeout

This command restores the soft timeout for secure HTTP sessions to the default value.

Format	**no ip http secure-session soft-timeout**
Mode	Privileged EXEC

ip http secure-port

This command is used to set the SSL port where port can be 1-65535 and the default is port 443.

Default	443
Format	**ip http secure-port** *<portid>*
Mode	Privileged EXEC

no ip http secure-port

This command is used to reset the SSL port to the default value.

Format	**no ip http secure-port**
Mode	Privileged EXEC

ip http secure-protocol

This command is used to set protocol levels (versions). The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

Default	SSL3 and TLS1
Format	**ip http secure-protocol** *[SSL3] [TLS1]*
Mode	Privileged EXEC

show ip http

This command displays the http settings for the switch.

Format	**show ip http**
Mode	Privileged EXEC

Term	*Definition*
HTTP Mode (Unsecure)	The unsecure HTTP server administrative mode.
Java Mode	The java applet administrative mode which applies to both secure and un-secure web connections.
Maximum Allowable HTTP Sessions	The number of allowable un-secure http sessions.
HTTP Session Hard Timeout	The hard timeout for un-secure http sessions in hours.

Term	*Definition*
HTTP Session Soft Timeout	The soft timeout for un-secure http sessions in minutes.
HTTP Mode (Secure)	The secure HTTP server administrative mode.
Secure Port	The secure HTTP server port number.
Secure Protocol Level(s)	The protocol level may have the values of SSL3, TSL1, or both SSL3 and TSL1.
Maximum Allowable HTTPS Sessions	The number of allowable secure http sessions.
HTTPS Session Hard Timeout	The hard timeout for secure http sessions in hours.
HTTPS Session Soft Timeout	The soft timeout for secure http sessions in minutes.
Certificate Present	Indicates whether the secure-server certificate files are present on the device.
Certificate Generation in Progress	Indicates whether certificate generation is currently in progress.

ACCESS COMMANDS

Use the commands in this section to close remote connections or to view information about connections to the system.

disconnect

Use the **disconnect** command to close HTTP, HTTPS, Telnet or SSH sessions. Use *all* to close all active sessions, or use *<session-id>* to specify the session ID to close. To view the possible values for *<session-id>*, use the **show loginsession** command.

Format **disconnect** *{<session_id> | all}*

Mode Privileged EXEC

show loginsession

This command displays current Telnet and serial port connections to the switch.

Format **show loginsession**

Mode Privileged EXEC

Term	*Definition*
ID	Login Session ID.
User Name	The name the user entered to log on to the system.
Connection From	IP address of the remote client machine or EIA-232 for the serial port connection.
Idle Time	Time this session has been idle.

Term	*Definition*
Session Time	Total time this session has been connected.
Session Type	Shows the type of session, which can be HTTP, HTTPS, telnet, serial, or SSH.

USER ACCOUNT COMMANDS

This section describes the commands you use to add, manage, and delete system users. Unified Switch software has two default users: admin and guest. The admin user can view and configure system settings, and the guest user can view settings.

Note: You cannot delete the admin user. There is only one user allowed with read/write privileges. You can configure up to five read-only users on the system.

users name

This command adds a new user account, if space permits. The account *<username>* can be up to eight characters in length. You can use alphanumeric characters as well as the dash (-) and underscore (_). You can define up to six user names.

Note: The *<username>* is not case sensitive when you add and delete users, and when the user logs in. However, when you use the *<username>* to set the user password, authentication, or encryption, you must enter the *<username>* in the same case you used when you added the user. To see the case of the *<username>*, enter the **show users** command.

Format **users name** *<username>*

Mode Global Config

no users name

This command removes a user account.

Format **no users name** *<username>*

Mode Global Config

Note: You cannot delete the “admin” user account.

users name unlock

Use this command to unlock a locked user account. Only a user with read/write access can re-activate a locked user account.

Format **users name** *<username>* **unlock**

Mode Global Config

users passwd

Use this command to change a password. Passwords are a maximum of 64 alphanumeric characters. If a user is authorized for authentication or encryption is enabled, the password length must be at least eight alphanumeric characters. The password is case sensitive. When you change a password, a prompt asks for the old password. If there is no password, press enter. You must enter the *<username>* in the same case you used when you added the user. To see the case of the *<username>*, enter the **show users** command.

Note: To specify a blank password in the configuration script, you must specify it as a space within quotes, for example, " ". For more information about creating configuration scripts, see "Configuration Scripting Commands" on page 517.

Default	no password
Format	**users passwd** *<username>*
Mode	Global Config

no users passwd

This command sets the password of an existing user to blank. When you change a password, a prompt asks for the old password. If there is no password, press enter.

Format	**no users passwd** *<username>*
Mode	Global Config

users passwd encrypted

This command allows the administrator to transfer local user passwords between devices without having to know the passwords. The *<password>* parameter must be exactly 128 hexadecimal characters. The user represented by the *<username>* parameter must be a pre-existing local user.

Format	**users passwd** *<username>* **encrypted** *<password>*
Mode	Global Config

users snmpv3 accessmode

This command specifies the snmpv3 access privileges for the specified login user. The valid accessmode values are **readonly** or **readwrite**. The *<username>* is the login user name for which the specified access mode applies. The default is **readwrite** for the "admin" user and **readonly** for all other users. You must enter the *<username>* in the same case you used when you added the user. To see the case of the *<username>*, enter the **show users** command.

Defaults	• admin - readwrite • other - readonly
Format	**users snmpv3 accessmode** *<username> {readonly | readwrite}*
Mode	Global Config

no users snmpv3 accessmode

This command sets the snmpv3 access privileges for the specified user as **readwrite** for the "admin" user and **readonly** for all other users. The *<username>* value is the user name for which the specified access mode will apply.

Format	**no users snmpv3 accessmode** *<username>*
Mode	Global Config

users snmpv3 authentication

This command specifies the authentication protocol to be used for the specified user. The valid authentication protocols are **none**, **md5** or **sha**. If you specify **md5** or **sha**, the login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The *<username>* is the user name associated with the authentication protocol. You must enter the *<username>* in the same case you used when you added the user. To see the case of the *<username>*, enter the **show users** command.

Default	no authentication
Format	**users snmpv3 authentication** *<username> {none | md5 | sha}*
Mode	Global Config

no users snmpv3 authentication

This command sets the authentication protocol to be used for the specified user to **none**. The *<username>* is the user name for which the specified authentication protocol is used.

Format	**no users snmpv3 authentication** *<username>*
Mode	Global Config

users snmpv3 encryption

This command specifies the encryption protocol used for the specified user. The valid encryption protocols are **des** or **none.**

If you select **des**, you can specify the required key on the command line. The encryption key must be 8 to 64 characters long. If you select the **des** protocol but do not provide a key, the user is prompted for the key. When you use the **des** protocol, the login password is also used as the snmpv3 encryption password, so it must be a minimum of eight characters. If you select **none**, you do not need to provide a key.

The *<username>* value is the login user name associated with the specified encryption. You must enter the *<username>* in the same case you used when you added the user. To see the case of the *<username>*, enter the **show users** command.

Default	no encryption
Format	**users snmpv3 encryption** *<username> {none | des[key]}*
Mode	Global Config

no users snmpv3 encryption

This command sets the encryption protocol to **none**. The *<username>* is the login user name for which the specified encryption protocol will be used.

Format **no users snmpv3 encryption** *<username>*

Mode Global Config

show users

This command displays the configured user names and their settings. This command is only available for users with Read/Write privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

Format **show users**

Mode Privileged EXEC

Term	*Definition*
User Name	The name the user enters to login using the serial port, Telnet or Web.
User Access Mode	Shows whether the user is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). As a factory default, the “admin” user has Read/Write access and the “guest” has Read Only access. There can only be one Read/Write user and up to five Read Only users.
SNMPv3 Access Mode	The SNMPv3 Access Mode. If the value is set to **ReadWrite,** the SNMPv3 user is able to set and retrieve parameters on the system. If the value is set to **ReadOnly,** the SNMPv3 user is only able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and Web access mode.
SNMPv3 Authentication	The authentication protocol to be used for the specified login user.
SNMPv3 Encryption	The encryption protocol to be used for the specified login user.

show users accounts

This command displays the local user status with respect to user account lockout and password aging.

Format **show users accounts**

Mode Privileged EXEC

Term	*Definition*
User Name	The local user account’s user name.
Access Mode	The user’s access level (read-only or read/write).
Lockout Status	Indicates whether the user account is locked out (true or false).
Password Expiry Date	The current password expiration date in date format.

passwd

This command allows the currently logged in user to change his or her password without having read/write privileges.

Format **password** *<cr>*
Mode User EXEC

passwords min-length

Use this command to enforce a minimum password length for local users. The value also applies to the enable password. The valid range is 8-64.

Default 8
Format **passwords min-length** *<8-64>*
Mode Global Config

no passwords min-length

Use this command to set the minimum password length to the default value.

Format **no passwords min-length**
Mode Global Config

passwords history

Use this command to set the number of previous passwords that shall be stored for each user account. When a local user changes his or her password, the user will not be able to reuse any password stored in password history. This ensures that users don't reuse their passwords often. The valid range is 0-10.

Default 0
Format **passwords history** *<0-10>*
Mode Global Config

no passwords history

Use this command to set the password history to the default value.

Format **no passwords history**
Mode Global Config

passwords aging

Use this command to implement aging on passwords for local users. When a user's password expires, the user will be prompted to change it before logging in again. The valid range is 1-365. The default is 0, or no aging.

Default 0
Format **passwords aging** *<1-365>*
Mode Global Config

no passwords aging

Use this command to set the password aging to the default value.

Format **no passwords aging**
Mode Global Config

passwords lock-out

Use this command to strengthen the security of the switch by locking user accounts that have failed login due to wrong passwords. When a lockout count is configured, a user that is logged in must enter the correct password within that count. Otherwise the user will be locked out from further switch access. Only a user with read/write access can re-activate a locked user account. Password lockout does not apply to logins from the serial console. The valid range is 1-5. The default is 0, or no lockout count enforced.

Default 0
Format **passwords lock-out** *<1-5>*
Mode Global Config

no passwords lock-out

Use this command to set the password lock-out count to the default value.

Format **no passwords lock-out**
Mode Global Config

show passwords configuration

Use this command to display the configured password management settings.

Format **show passwords configuration**
Mode Privileged EXEC

Term	*Definition*
Minimum Password Length	Minimum number of characters required when changing passwords.
Password History	Number of passwords to store for reuse prevention.
Password Aging	Length in days that a password is valid.
Lockout Attempts	Number of failed password login attempts before lockout.

write memory

Use this command to save running configuration changes to NVRAM so that the changes you make will persist across a reboot. This command is the same as `copy system:running config nvram:startup-config`.

Format **write memory**
Mode Privileged EXEC

SNMP COMMANDS

This section describes the commands you use to configure Simple Network Management Protocol (SNMP) on the switch. You can configure the switch to act as an SNMP agent so that it can communicate with SNMP managers on your network.

snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network. The range for *<name>*, *<loc>* and *<con>* is from 1 to 31 alphanumeric characters.

Default	none
Format	**snmp-server** *{sysname <name> | location <loc> | contact <con>}*
Mode	Global Config

snmp-server community

This command adds (and names) a new SNMP community. A community *<name>* is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of *<name>* can be up to 16 case-sensitive characters.

Note: Community names in the SNMP Community Table must be unique. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Default	• Public and private, which you can rename. • Default values for the remaining four community names are blank.
Format	**snmp-server community** *<name>*
Mode	Global Config

no snmp-server community

This command removes this community name from the table. The *<name>* is the community name to be deleted.

Format	**no snmp-server community** *<name>*
Mode	Global Config

snmp-server community ipaddr

This command sets a client IP address for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses. The name is the applicable community name.

Default	0.0.0.0
Format	**snmp-server community ipaddr** *<ipaddr> <name>*
Mode	Global Config

no snmp-server community ipaddr

This command sets a client IP address for an SNMP community to 0.0.0.0. The name is the applicable community name.

Format **no snmp-server community ipaddr** *<name>*

Mode Global Config

snmp-server community ipmask

This command sets a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP address value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 255.255.255.255 will allow access from only one station, and will use that machine's IP address for the client IP address. A value of 0.0.0.0 will allow access from any IP address. The name is the applicable community name.

Default 0.0.0.0

Format **snmp-server community ipmask** *<ipmask> <name>*

Mode Global Config

no snmp-server community ipmask

This command sets a client IP mask for an SNMP community to 0.0.0.0. The name is the applicable community name. The community name may be up to 16 alphanumeric characters.

Format **no snmp-server community ipmask** *<name>*

Mode Global Config

snmp-server community mode

This command activates an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the switch according to its access right. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

Default
- private and public communities - enabled
- other four - disabled

Format **snmp-server community mode** *<name>*

Mode Global Config

no snmp-server community mode

This command deactivates an SNMP community. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

Format **no snmp-server community mode** *<name>*

Mode Global Config

snmp-server community ro

Format	`snmp-server community ro <name>`
Mode	Global Config

This command restricts access to switch information. The access mode is read-only (also called public).

snmp-server community rw

This command restricts access to switch information. The access mode is read/write (also called private).

Format	`snmp-server community rw <name>`
Mode	Global Config

snmp-server enable traps violation

This command enables the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port.

Note: For other port security commands, see “Protected Ports Commands” on page 47.

Default	disabled
Format	`snmp-server enable traps violation`
Mode	Interface Config

no snmp-server enable traps violation

This command disables the sending of new violation traps.

Format	`no snmp-server enable traps violation`
Mode	Interface Config

snmp-server enable traps

This command enables the Authentication failure trap.

Default	enabled
Format	`snmp-server enable traps`
Mode	Global Config

no snmp-server enable traps

This command disables the Authentication failure trap.

Format	`no snmp-server enable traps`
Mode	Global Config

snmp-server enable traps linkmode

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. See “snmp trap link-status” on page 501.

Default enabled

Format `snmp-server enable traps linkmode`

Mode Global Config

no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

Format `no snmp-server enable traps linkmode`

Mode Global Config

snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or Telnet) and there is an existing terminal interface session.

Default enabled

Format `snmp-server enable traps multiusers`

Mode Global Config

no snmp-server enable traps multiusers

This command disables Multiple User traps.

Format `no snmp-server enable traps multiusers`

Mode Global Config

snmp-server enable traps stpmode

This command enables the sending of new root traps and topology change notification traps.

Default enabled

Format `snmp-server enable traps stpmode`

Mode Global Config

no snmp-server enable traps stpmode

This command disables the sending of new root traps and topology change notification traps.

Format `no snmp-server enable traps stpmode`

Mode Global Config

snmptrap

This command adds an SNMP trap receiver. The maximum length of *<name>* is 16 case-sensitive alphanumeric characters. The *<snmpversion>* is the version of SNMP. The version parameter options are snmpv1 or snmpv2.

Example: The following shows an example of the CLI command.

```
(admin #) snmptrap mytrap 10.12.41.2
```

Note: The *<name>* parameter does not need to be unique, however; the *<name>* and *<ipaddr>* pair must be unique. Multiple entries can exist with the same *<name>*, as long as they are associated with a different *<ipaddr>*. The reverse scenario is also acceptable. The *<name>* is the community name used when sending the trap to the receiver, but the *<name>* is not directly associated with the SNMP Community Table, See "snmp-server community" on page 496.

Default	snmpv2
Format	**snmptrap** *<name> <ipaddr> [snmpversion <snmpversion>]*
Mode	Global Config

no snmptrap

This command deletes trap receivers for a community.

Format	**no snmptrap** *<name> <ipaddr>*
Mode	Global Config

snmptrap snmpversion

This command modifies the SNMP version of a trap. The maximum length of *<name>* is 16 case-sensitive alphanumeric characters. The *<snmpversion>* parameter options are snmpv1 or snmpv2.

Note: This command does not support a "no" form.

Default	snmpv2
Format	**snmptrap snmpversion** *<name> <ipaddr> <snmpversion>*
Mode	Global Config

snmptrap ipaddr

This command assigns an IP address to a specified community name. The maximum length of name is 16 case-sensitive alphanumeric characters.

Note: IP addresses in the SNMP trap receiver table must be unique. If you make multiple entries using the same IP address, the first entry is retained and processed. All duplicate entries are ignored.

Format	**snmptrap ipaddr** *<name> <ipaddrold> <ipaddrnew>*
Mode	Global Config

snmptrap mode

This command activates or deactivates an SNMP trap. Enabled trap receivers are active (able to receive traps). Disabled trap receivers are inactive (not able to receive traps).

Format **snmptrap mode** *<name> <ipaddr>*

Mode Global Config

no snmptrap mode

This command deactivates an SNMP trap. Disabled trap receivers are unable to receive traps.

Format **no snmptrap mode** *<name> <ipaddr>*

Mode Global Config

snmp trap link-status

This command enables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled. See “snmp-server enable traps linkmode” on page 499.

Format **snmp trap link-status**

Mode Interface Config

no snmp trap link-status

This command disables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled.

Format **no snmp trap link-status**

Mode Interface Config

snmp trap link-status all

This command enables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled. See “snmp-server enable traps linkmode” on page 499.

Format **snmp trap link-status all**

Mode Global Config

no snmp trap link-status all

This command disables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled. See “snmp-server enable traps linkmode” on page 499.

Format	`no snmp trap link-status all`
Mode	Global Config

show snmpcommunity

This command displays SNMP community information. Six communities are supported. You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.

The SNMP agent of the switch complies with SNMP Versions 1, 2 or 3. For more information about the SNMP specification, see the SNMP RFCs. The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

Format	`show snmpcommunity`
Mode	Privileged EXEC

Term	*Definition*
SNMP Community Name	The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
Client IP Address	An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP address. Note: If the Subnet Mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.
Client IP Mask	A mask to be ANDed with the requesting entity's IP address before comparison with IP address. If the result matches with IP address then the address is an authenticated IP address. For example, if the IP address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, i.e. the incoming IP address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0.
Access Mode	The access level for this community string.
Status	The status of this community access entry.

show snmptrap

This command displays SNMP trap receivers. Trap messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network. Six trap receivers are simultaneously supported.

Format	`show snmptrap`
Mode	Privileged EXEC

Term	*Definition*
SNMP Trap Name	The community string of the SNMP trap packet sent to the trap manager. The string is case sensitive and can be up to 16 alphanumeric characters.
IP Address	The IPv4 address to receive SNMP traps from this device.
SNMP Version	SNMPv2
Mode	The receiver's status (enabled or disabled).

Example: The following shows an example of the CLI command.

```
(DWS-4026) #show snmptrap

SNMP Trap Name      IP Address      IPv6 Address          SNMP Version  Status

------------------- --------------- --------------------- ------------- ---------

MyTrap              192.168.1.100                         snmpv2        Disable
```

show trapflags

This command displays trap conditions. You can configure which traps the switch generates by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the SNMP agent on the switch sends the trap to all enabled trap receivers. You do not have to reset the switch to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format `show trapflags`

Mode Privileged EXEC

Term	*Definition*
Authentication Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
Multiple Users Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port).
Spanning Tree Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps are sent.
ACL Traps	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.
Global Wireless Trap Flag	Indicates whether Unified Switch SNMP traps are globally enabled.
Captive Portal Flag	Indicates whether Captive Portal SNMP traps are globally enabled.

RADIUS COMMANDS

This section describes the commands you use to configure the switch to use a Remote Authentication Dial-In User Service (RADIUS) server on your network for authentication and accounting.

authorization network radius

Use this command to enable the switch to accept VLAN assignment by the radius server.

Default	disable
Format	`authorization network radius`
Mode	Global Config

no authorization network radius

Use this command to disable the switch to accept VLAN assignment by the radius server.

Format	`no authorization network radius`
Mode	Global Config

radius accounting mode

This command is used to enable the RADIUS accounting function on the Unified Switch.

Default	disabled
Format	`radius accounting mode`
Mode	Global Config

no radius accounting mode

This command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

Format	`no radius accounting mode`
Mode	Global Config

radius server attribute

This command specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests. If the specific IP address is configured while enabling this attribute, the RADIUS client uses that IP address while sending NAS-IP-Address attribute in RADIUS communication.

Format	`radius server attribute <4>` *[<ipaddr>]*
Mode	Global Config

Term	Definition
4	NAS-IP-Address attribute to be used in RADIUS requests.
ipaddr	The IPv4 address of the server.

no radius server attribute

The no version of this command disables the NAS-IP-Address attribute global parameter for RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IP-Address attribute in RADIUS requests.

Format **no radius server attribute <4>** *[<ipaddr>]*

Mode Global Config

Example: The following shows an example of the command.

```
(DWS-4026) (Config) #radius server attribute 4  192.168.37.60
(DWS-4026) (Config) #radius server attribute 4
```

radius server host

This command configures the IP address or DNS name to use for communicating with the RADIUS server of a selected server type. While configuring the IP address or DNS name for the authenticating or accounting servers, you can also configure the port number and server name. If the authenticating and accounting servers are configured without a name, the command uses the Default_RADIUS_Auth_Server and Default_RADIUS_Acct_Server as the default names, respectively. The same name can be configured for more than one authenticating servers and the name should be unique for accounting servers. The RADIUS client allows the configuration of a maximum 32 authenticating and accounting servers.

If you use the *<auth>* parameter, the command configures the IP address or hostname to use to connect to a RADIUS authentication server. You can configure up to 32 servers per RADIUS client. If the maximum number of configured servers is reached, the command fails until you remove one of the servers by issuing the “no” form of the command. If you use the optional *<port>* parameter, the command configures the UDP port number to use when connecting to the configured RADIUS server. The *<port>* number range is 1 - 65535, with 1812 being the default value.

Note: To re-configure a RADIUS authentication server to use the default UDP *<port>*, set the *<port>* parameter to 1812.

If you use the *<acct>* token, the command configures the IP address or hostname to use for the RADIUS accounting server. You can only configure one accounting server. If an accounting server is currently configured, use the “no” form of the command to remove it from the configuration. The IP address or hostname you specify must match that of a previously configured accounting server. If you use the optional *<port>* parameter, the command configures the UDP port to use when connecting to the RADIUS accounting server. If a *<port>* is already configured for the accounting server, the new *<port>* replaces the previously configured *<port>*. The *<port>* must be a value in the range 0 - 65535, with 1813 being the default.

Note: To re-configure a RADIUS accounting server to use the default UDP *<port>*, set the *<port>* parameter to 1813.

Format **radius server host** *{auth | acct} {<ipaddr|dnsname>} [name <servername>] [port <0-65535>]*

Mode Global Config

Field	*Description*
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
0-65535	The port number to use to connect to the specified RADIUS server.
servername	The alias name to identify the server.

no radius server host

The no version of this command deletes the configured server entry from the list of configured RADIUS servers. If the RADIUS authenticating server being removed is the active server in the servers that are identified by the same server name, then the RADIUS client selects another server for making RADIUS transactions. If the 'auth' token is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the 'acct' token is used, the previously configured RADIUS accounting server is removed from the configuration. The *<ipaddr|dnsname>* parameter must match the IP address or dns name of the previously configured RADIUS authentication / accounting server.

Format **no radius server host** *{auth | acct} {<ipaddr|dnsname>}*

Mode Global Config

Example: The following shows an example of the command.

```
(DWS-4026) (Config) #radius server host acct 192.168.37.60
(DWS-4026) (Config) #radius server host acct 192.168.37.60 port 1813
(DWS-4026) (Config) #radius server host auth 192.168.37.60 name
Network1_RADIUS_Auth_Server port 1813

(DWS-4026) (Config) #radius server host acct 192.168.37.60 name Network2_RADIUS_Auth_Server
(DWS-4026) (Config) #no radius server host acct 192.168.37.60
```

radius server key

This command configures the key to be used in RADIUS client communication with the specified server. Depending on whether the 'auth' or 'acct' token is used, the shared secret is configured for the RADIUS authentication or RADIUS accounting server. The IP address or hostname provided must match a previously configured server. When this command is executed, the secret is prompted.

Text-based configuration supports Radius server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the show running config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Note: The secret must be an alphanumeric value not exceeding 16 characters.

Format **radius server key** *{auth | acct} {<ipaddr|dnsname>} encrypted <password>*

Mode Global Config

Field	*Description*
ipaddr	The IP address of the server.

Field	Description
dnsname	The DNS name of the server.
password	The password in encrypted format.

Example: The following shows an example of the CLI command.

```
radius server key acct 10.240.4.10 encrypted <encrypt-string>
```

radius server msgauth

This command enables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format **radius server msgauth** *<ipaddr|dnsname>*

Mode Global Config

Field	Description
ip addr	The IP address of the server.
dnsname	The DNS name of the server.

no radius server msgauth

The no version of this command disables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format **no radius server msgauth** *<ipaddr|dnsname>*

Mode Global Config

radius server primary

This command specifies a configured server that should be the primary server in the group of servers which have the same server name. Multiple primary servers can be configured for each number of servers that have the same name. When the RADIUS client has to perform transactions with an authenticating RADIUS server of specified name, the client uses the primary server that has the specified server name by default. If the RADIUS client fails to communicate with the primary server for any reason, the client uses the backup servers configured with the same server name. These backup servers are identified as the Secondary type.

Format **radius server primary** {*<ipaddr|dnsname>*}

Mode Global Config

Field	Description
ip addr	The IP address of the RADIUS Authenticating server.
dnsname	The DNS name of the server.

radius server retransmit

This command configures the global parameter for the RADIUS client that specifies the number of transmissions of the messages to be made before attempting the fall back server upon unsuccessful communication with the current RADIUS authenticating server. When the maximum number of retries are exhausted for the RADIUS accounting server and no response is received, the client does not communicate with any other server.

Default 4

Format **radius server retransmit** *<retries>*

Mode Global Config

Field	*Description*
retries	The maximum number of transmission attempts in the range of 1 to 15.

no radius server retransmit

The no version of this command sets the value of this global parameter to the default value.

Format **no radius server retransmit**

Mode Global Config

radius server timeout

This command configures the global parameter for the RADIUS client that specifies the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

Default 5

Format **radius server timeout** *<seconds>*

Mode Global Config

Field	*Description*
retries	Maximum number of transmission attempts in the range <1-30>.

no radius server timeout

The no version of this command sets the timeout global parameter to the default value.

Format **no radius server timeout**

Mode Global Config

show radius

This command displays the values configured for the global parameters of the RADIUS client.

Format `show radius`

Mode Privileged EXEC

Term	*Definition*
Number of Configured Authentication Servers	The number of RADIUS Authentication servers that have been configured.
Number of Configured Accounting Servers	The number of RADIUS Accounting servers that have been configured.
Number of Named Authentication Server Groups	The number of configured named RADIUS server groups.
Number of Named Accounting Server Groups	The number of configured named RADIUS server groups.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Time Duration	The configured timeout value, in seconds, for request re-transmissions.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in the NAS-IP-Address attribute to be used in RADIUS requests.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show radius

      Number of Configured Authentication Servers..... 32
      Number of Configured Accounting Servers......... 32
      Number of Named Authentication Server Groups.... 15
      Number of Named Accounting Server Groups........ 3
      Number of Retransmits........................... 4
      Time Duration................................... 10
      RADIUS Accounting Mode.......................... Disable
      RADIUS Attribute 4 Mode......................... Enable
      RADIUS Attribute 4 Value ....................... 192.168.37.60
```

show radius servers

This command displays the summary and details of RADIUS authenticating servers configured for the RADIUS client.

Format `show radius servers [ { <ipaddr | dnsname> | name [<servername> ] } ]`

Mode Privileged EXEC

Field	*Description*
ipaddr	The IP address of the authenticating server.
dnsname	The DNS name of the authenticating server.
servername	The alias name to identify the server.
Current	The * symbol preceeding the server host address specifies that the server is currently active.
Host Address	The IP address of the host.
Server Name	The name of the authenticating server.
Port	The port used for communication with the authenticating server.
Type	Specifies whether this server is a primary or secondary type.
Current Host Address	The IP address of the currently active authenticating server.
Secret Configured	Yes or No Boolean value that indicates whether this server is configured with a secret.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Message Authenticator	A global parameter to indicate whether the Message Authenticator attribute is enabled or disabled.
Time Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in NAS-IP-Address attribute used in RADIUS requests.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show radius servers

Cur  Host Address              Server Name                      Port  Type
rent
---- ----------------------- -------------------------------- ----- ----------
  *   192.168.37.200           Network1_RADIUS_Server           1813  Primary
     192.168.37.201           Network2_RADIUS_Server           1813  Secondary
     192.168.37.202           Network3_RADIUS_Server           1813  Primary
     192.168.37.203           Network4_RADIUS_Server           1813  Secondary

(DWS-4026) #show radius servers name

Current Host Address     Server Name                        Type
----------------------- ---------------------------------- ----------192.168.37.200
Network1_RADIUS_Server            Secondary
192.168.37.201           Network2_RADIUS_Server            Primary
192.168.37.202           Network3_RADIUS_Server            Secondary
192.168.37.203           Network4_RADIUS_Server            Primary

(DWS-4026) #show radius servers name Default_RADIUS_Server

Server Name.............................. Default_RADIUS_Server
Host Address............................. 192.168.37.58
Secret Configured....................... No
```



```
   Message Authenticator ................. Enable
   Number of Retransmits.................. 4
   Time Duration.......................... 10
   RADIUS Accounting Mode................. Disable
   RADIUS Attribute 4 Mode................ Enable
   RADIUS Attribute 4 Value .............. 192.168.37.60

   (DWS-4026) #show radius servers 192.168.37.58

   Server Name............................ Default_RADIUS_Server
   Host Address........................... 192.168.37.58
   Secret Configured...................... No
   Message Authenticator ................. Enable
   Number of Retransmits.................. 4
   Time Duration.......................... 10
   RADIUS Accounting Mode................. Disable
   RADIUS Attribute 4 Mode................ Enable
RADIUS Attribute 4 Value .............. 192.168.37.60
```

show radius accounting

This command displays a summary of configured RADIUS accounting servers.

Format **show radius accounting name** *[<servername>]*

Mode Privileged EXEC

Field	*Description*
servername	An alias name to identify the server.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

Term	*Definition*
Host Address	The IP address of the host.
Server Name	The name of the accounting server.
Port	The port used for communication with the accounting server.
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show radius accounting name

Host Address            Server Name                       Port     Secret
                                                                   Configured
---------------------- ---------------------------------- -------- -----------
192.168.37.200          Network1_RADIUS_Server            1813     Yes
192.168.37.201          Network2_RADIUS_Server            1813     No
192.168.37.202          Network3_RADIUS_Server            1813     Yes
192.168.37.203          Network4_RADIUS_Server            1813     No
```

```
(DWS-4026) #show radius accounting name Default_RADIUS_Server

Server Name..............................  Default_RADIUS_Server
Host Address.............................  192.168.37.200
RADIUS Accounting Mode...................  Disable
Port ....................................  1813
Secret Configured .......................  Yes
```

show radius accounting statistics

This command displays a summary of statistics for the configured RADIUS accounting servers.

Format **show radius accounting statistics {***<ipaddr|dnsname> | name <servername>}*

Mode Privileged EXEC

Term	*Definition*
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
servername	The alias name to identify the server.
RADIUS Accounting Server Name	The name of the accounting server.
Server Host Address	The IP address of the host.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
Retransmission	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show radius accounting statistics 192.168.37.200
```



```
RADIUS Accounting Server Name.................. Default_RADIUS_Server
Host Address................................... 192.168.37.200
Round Trip Time................................ 0.00
Requests....................................... 0
Retransmissions................................ 0
Responses...................................... 0
Malformed Responses............................ 0
Bad Authenticators............................. 0
Pending Requests............................... 0
Timeouts....................................... 0
Unknown Types.................................. 0
Packets Dropped................................ 0

(DWS-4026) #show radius accounting statistics name Default_RADIUS_Server

RADIUS Accounting Server Name.................. Default_RADIUS_Server
Host Address................................... 192.168.37.200
Round Trip Time................................ 0.00
Requests....................................... 0
Retransmissions................................ 0
Responses...................................... 0
Malformed Responses............................ 0
Bad Authenticators............................. 0
Pending Requests............................... 0
Timeouts....................................... 0
Unknown Types.................................. 0
Packets Dropped................................ 0
```

show radius statistics

This command displays the summary statistics of configured RADIUS Authenticating servers.

Format **show radius statistics** {*<ipaddr|dnsname> | name <servername>*}

Mode Privileged EXEC

Term	*Definition*
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
servername	The alias name to identify the server.
RADIUS Server Name	The name of the authenticating server.
Server Host Address	The IP address of the host.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.

Term	*Definition*
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of packets of unknown type that were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

Example: The following shows example CLI display output for the command.

```
(DWS-4026) #show radius statistics 192.168.37.200

RADIUS Server Name..................................... Default_RADIUS_Server
Server Host Address.................................... 192.168.37.200
Access Requests........................................ 0.00
Access Retransmissions................................. 0
Access Accepts......................................... 0
Access Rejects......................................... 0
Access Challenges...................................... 0
Malformed Access Responses............................. 0
Bad Authenticators..................................... 0
Pending Requests....................................... 0
Timeouts............................................... 0
Unknown Types.......................................... 0
Packets Dropped........................................ 0

(DWS-4026) #show radius statistics name Default_RADIUS_Server

RADIUS Server Name..................................... Default_RADIUS_Server
Server Host Address.................................... 192.168.37.200
Access Requests........................................ 0.00
Access Retransmissions................................. 0
Access Accepts......................................... 0
Access Rejects......................................... 0
Access Challenges...................................... 0
Malformed Access Responses............................. 0
Bad Authenticators..................................... 0
Pending Requests....................................... 0
Timeouts............................................... 0
Unknown Types.......................................... 0
Packets Dropped........................................ 0
```


TACACS+ COMMANDS

TACACS+ provides access control for networked devices via one or more centralized servers. Similar to RADIUS, this protocol simplifies authentication by making use of a single database that can be shared by many clients on a large network. TACACS+ is based on the TACACS protocol (described in RFC1492) but additionally provides for separate authentication, authorization, and accounting services. The original protocol was UDP based with messages passed in clear text over the network; TACACS+ uses TCP to ensure reliable delivery and a shared key configured on the client and daemon server to encrypt all messages.

tacacs-server host

Use the **tacacs-server host** command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. The *<ip-address|hostname>* parameter is the IP address or hostname of the TACACS+ server. To specify multiple hosts, multiple **tacacs-server host** commands can be used.

Format **tacacs-server host** *<ip-address|hostname>*

Mode Global Config

no tacacs-server host

Use the **no tacacs-server host** command to delete the specified hostname or IP address. The *<ip-address|hostname>* parameter is the IP address of the TACACS+ server.

Format **no tacacs-server host** *<ip-address|hostname>*

Mode Global Config

tacacs-server key

Use the **tacacs-server key** command to set the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The *<key-string>* parameter has a range of 0 - 128 characters and specifies the authentication and encryption key for all TACACS communications between the switch and the TACACS+ server. This key must match the key used on the TACACS+ daemon.

Text-based configuration supports TACACS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the show running config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format **tacacs-server key** [*<key-string>* | *encrypted <key-string>]*

Mode Global Config

no tacacs-server key

Use the **no tacacs-server key** command to disable the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The *<key-string>* parameter has a range of 0 - 128 characters This key must match the key used on the TACACS+ daemon.

Format **no tacacs-server key** *<key-string>*

Mode Global Config

tacacs-server timeout

Use the **tacacs-server timeout** command to set the timeout value for communication with the TACACS+ servers. The *<timeout>* parameter has a range of 1-30 and is the timeout value in seconds.

Default	5
Format	**tacacs-server timeout** *<timeout>*
Mode	Global Config

no tacacs-server timeout

Use the **no tacacs-server timeout** command to restore the default timeout value for all TACACS servers.

Format	**no tacacs-server timeout**
Mode	Global Config

key

Use the **key** command in TACACS Configuration mode to specify the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the key used on the TACACS daemon. The *<key-string>* parameter specifies the key name. For an empty string use " ". (Range: 0 - 128 characters).

Text-based configuration supports TACACS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the show running config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format	**key** [*<key-string>* | *encrypted <key-string>]*
Mode	TACACS Config

port

Use the **port** command in TACACS Configuration mode to specify a server port number. The server *<port-number>* range is 0 - 65535.

Default	49
Format	**port** *<port-number>*
Mode	TACACS Config

priority

Use the **priority** command in TACACS Configuration mode to specify the order in which servers are used, where 0 (zero) is the highest priority. The *<priority>* parameter specifies the priority for servers. The highest priority is 0 (zero), and the range is 0 - 65535.

Default	0
Format	**priority** *<priority>*
Mode	TACACS Config

timeout

Use the **timeout** command in TACACS Configuration mode to specify the timeout value in seconds. If no timeout value is specified, the global value is used. The *<timeout>* parameter has a range of 1-30 and is the timeout value in seconds.

Format	**timeout** *<timeout>*
Mode	TACACS Config

show tacacs

Use the **show tacacs** command to display the configuration and statistics of a TACACS+ server.

Format	**show tacacs** *[<ip-address|hostname>]*
Mode	Privileged EXEC

Term	*Definition*
IP address or Hostname	The IP address or hostname of the configured TACACS+ server.
Port	The configured TACACS+ server port number.
TimeOut	The timeout in seconds for establishing a TCP connection.
Priority	The preference order in which TACACS+ servers are contacted. If a server connection fails, the next highest priority server is contacted.

CONFIGURATION SCRIPTING COMMANDS

Configuration Scripting allows you to generate text-formatted script files representing the current configuration of a system. You can upload these configuration script files to a PC or UNIX system and edit them. Then, you can download the edited files to the system and apply the new configuration. You can apply configuration scripts to one or more switches with no or minor modifications.

Use the **show running-config** command (see "show running-config" on page 421) to capture the running configuration into a script. Use the **copy** command (see "copy" on page 434) to transfer the configuration script to or from the switch.

You should use scripts on systems with default configuration; however, you are not prevented from applying scripts on systems with non-default configurations.

Scripts must conform to the following rules:

- The file extension must be ".scr".
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

You can type single-line annotations at the command prompt to use when you write test or configuration scripts to improve script readability. The exclamation point (!) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line, and all input following this character is ignored. Any command line that begins with the "!" character is recognized as a comment line and ignored by the parser.

The following lines show an example of a script:

```
! Script file for displaying management access

show telnet !Displays the information about remote connections

! Display information about direct connections

show serial

! End of the script file!
```

Note: To specify a blank password for a user in the configuration script, you must specify it as a space within quotes. For example, to change the password for user jane from a blank password to *hello*, the script entry is as follows:

```
users passwd jane
" "
hello
hello
```

script apply

This command applies the commands in the script to the switch. The *<scriptname>* parameter is the name of the script to apply.

Format	**script apply** *<scriptname>*
Mode	Privileged EXEC

script delete

This command deletes a specified script where the *<scriptname>* parameter is the name of the script to delete. The *<all>* option deletes all the scripts present on the switch.

Format	**script delete** *{<scriptname> | all}*
Mode	Privileged EXEC

script list

This command lists all scripts present on the switch as well as the remaining available space.

Format	**script list**
Mode	Global Config

Term	*Definition*
Configuration Script	Name of the script.
Size	Privileged EXEC

script show

This command displays the contents of a script file, which is named *<scriptname>*.

Format **script show** *<scriptname>*
Mode Privileged EXEC

Term	*Definition*
Output Format	**line** *<number>*: *<line contents>*

script validate

This command validates a script file by parsing each line in the script file where *<scriptname>* is the name of the script to validate.The validate option is intended to be used as a tool for script development. Validation identifies potential problems. It might not identify all problems with a given script on any given device.

Format **script validate** *<scriptname>*
Mode Privileged EXEC

PRE-LOGIN BANNER AND SYSTEM PROMPT COMMANDS

This section describes the commands you use to configure the pre-login banner and the system prompt. The pre-login banner is the text that displays before you login at the **User:** prompt.

copy (pre-login banner)

The **copy** command includes the option to upload or download the CLI Banner to or from the switch. You can specify local URLs by using TFTP, Xmodem, Ymodem, or Zmodem.

Default none
Format **copy** <tftp://<ipaddr>/<filepath>/<filename>> **nvram:clibanner**

copy nvram:clibanner <tftp://<ipaddr>/<filepath>/<filename>>
Mode Privileged EXEC

set prompt

This command changes the name of the prompt. The length of name may be up to 64 alphanumeric characters.

Format **set prompt** *<prompt_string>*
Mode Privileged EXEC

Section 10: Unified Switch Log Messages

This section lists common log messages that are provided by Unified Switch , along with information regarding the cause of each message. There is no specific action that can be taken per message. When there is a problem being diagnosed, a set of these messages in the event log, along with an understanding of the system configuration and details of the problem) will assist D-Link in determining the root cause of such a problem.

Note: This section is not a complete list of all syslog messages.

The Log Messages section includes the following subsections:

CORE

Table 12: BSP Log Messages

Component	*Message*	*Cause*
BSP	Event(0xaaaaaaaa)	Switch has restarted.
BSP	Starting code...	BSP initialization complete, starting Unified Switch application.

Table 13: NIM Log Messages

Component	*Message*	*Cause*
NIM	NIM: L7_ATTACH out of order for intIfNum(x) unit x slot x port x	Interface creation out of order.
NIM	NIM: Failed to find interface at unit x slot x port x for event(x)	There is no mapping between the USP and Interface number.
NIM	NIM: L7_DETACH out of order for intIfNum(x) unit x slot x port x	Interface creation out of order.
NIM	NIM: L7_DELETE out of order for intIfNum(x) unit x slot x port x	Interface creation out of order.

Table 13: NIM Log Messages (Cont.)

Component	Message	Cause
NIM	NIM: event(x),intf(x),component(x), in wrong phase	An event was issued to NIM during the wrong configuration phase (probably Phase 1, 2, or WMU).
NIM	NIM: Failed to notify users of interface change	Event was not propagated to the system.
NIM	NIM: failed to send message to NIM message Queue.	NIM message queue full or non-existent.
NIM	NIM: Failed to notify the components of L7_CREATE event	Interface not created.
NIM	NIM: Attempted event (x), on USP x.x.x before phase 3	A component issued an interface event during the wrong initialization phase.
NIM	NIM: incorrect phase for operation	An API call was made during the wrong initialization phase.
NIM	NIM: Component(x) failed on event(x) for intIfNum(x)	A component responded with a fail indication for an interface event.
NIM	NIM: Timeout event(x), intIfNum(x) remainingMask = xxxx	A component did not respond before the NIM timeout occurred.

Table 14: System Log Messages

Component	Message	Cause
SYSTEM	Configuration file fastpath.cfg size is 0 (zero) bytes	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	could not separate SYSAPI_CONFIG_FILENAME	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	Building defaults for file <file name> version <version num>	Configuration did not exist or could not be read for the specified feature or file. Default configuration values will be used. The file name and version are indicated.
SYSTEM	File <filename>: same version (version num) but the sizes (<version size>-><expected version size) differ	The configuration file which was loaded was of a different size than expected for the version number. This message indicates the configuration file needed to be migrated to the version number appropriate for the code image. This message may appear after upgrading the code image to a more current release.
SYSTEM	Migrating config file <filename> from version <version num> to <version num>	The configuration file identified was migrated from a previous version number. Both the old and new version number are specified. This message may appear after upgrading the code image to a more current release.
SYSTEM	Building Defaults	Configuration did not exist or could not be read for the specified feature. Default configuration values will be used.

Table 14: System Log Messages (Cont.)

Component	Message	Cause
SYSTEM	sysapiCfgFileGet failed size = <expected size of file> version = <expected version>	Configuration did not exist or could not be read for the specified feature. This message is usually followed by a message indicating that default configuration values will be used.

UTILITIES

Table 15: Trap Mgr Log Message

Component	Message	Cause
Trap Mgr	Link Up/Down: slot/port	An interface changed link state.

Table 16: DHCP Filtering Log Messages

Component	Message	Cause
DHCP Filtering	Unable to create r/w lock for DHCP Filtering	Unable to create semaphore used for dhcp filtering configuration structure.
DHCP Filtering	Failed to register with nv Store.	Unable to register save and restore functions for configuration save.
DHCP Filtering	Failed to register with NIM	Unable to register with NIM for interface callback functions.
DHCP Filtering	Error on call to sysapiCfgFileWrite file	Error on trying to save configuration.

Table 17: NVStore Log Messages

Component	Message	Cause
NVStore	Building defaults for file XXX	A component's configuration file does not exist or the file's checksum is incorrect so the component's default configuration file is built.
NVStore	Error on call to osapiFsWrite routine on file XXX	Either the file cannot be opened or the OS's file I/O returned an error trying to write to the file.
NVStore	File XXX corrupted from file system. Checksum mismatch.	The calculated checksum of a component's configuration file in the file system did not match the checksum of the file in memory.
NVStore	Migrating config file XXX from version Y to Z	A configuration file version mismatch was detected so a configuration file migration has started.

Table 18: RADIUS Log Messages

Component	Message	Cause
RADIUS	RADIUS: Invalid data length - xxx	The RADIUS Client received an invalid message from the server.

Table 18: RADIUS Log Messages (Cont.)

Component	Message	Cause
RADIUS	RADIUS: Failed to send the request	A problem communicating with the RADIUS server.
RADIUS	RADIUS: Failed to send all of the request	A problem communicating with the RADIUS server during transmit.
RADIUS	RADIUS: Could not get the Task Sync semaphore!	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Buffer is too small for response processing	RADIUS Client attempted to build a response larger than resources allow.
RADIUS	RADIUS: Could not allocate accounting requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Could not allocate requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: osapiSocketRecvFrom returned error	Error while attempting to read data from the RADIUS server.
RADIUS	RADIUS: Accounting-Response failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: User (xxx) needs to respond for challenge	An unexpected challenge was received for a configured user.
RADIUS	RADIUS: Could not allocate a buffer for the packet	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Access-Challenge failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to validate Message-Authenticator, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Access-Accpet failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Invalid packet length – xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Response is missing Message-Authenticator, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Server address doesn't match configured server	RADIUS Client received a server response from an unconfigured server.

Table 19: TACACS+ Log Messages

Component	Message	Cause
TACACS+	TACACS+: authentication error, no server to contact	TACACS+ request needed, but no servers are configured.
TACACS+	TACACS+: connection failed to server x.x.x.x	TACACS+ request sent to server x.x.x.x but no response was received.
TACACS+	TACACS+: no key configured to encrypt packet for server x.x.x.x	No key configured for the specified server.
TACACS+	TACACS+: received invalid packet type from server.	Received packet type that is not supported.
TACACS+	TACACS+: invalid major version in received packet.	Major version mismatch.
TACACS+	TACACS+: invalid minor version in received packet.	Minor version mismatch.

Table 20: LLDP Log Message

Component	Message	Cause
LLDP	lldpTask(): invalid message type:xx. xxxxxx:xx	Unsupported LLDP packet received.

Table 21: SNTP Log Message

Component	Message	Cause
SNTP	SNTP: system clock synchronized on %s UTC	Indicates that SNTP has successfully synchronized the time of the box with the server.

MANAGEMENT

Table 22: EmWeb Log Messages

Component	Message	Cause
EmWeb	EMWEB (Telnet): Max number of Telnet login sessions exceeded	A user attempted to connect via telnet when the maximum number of telnet sessions were already active.
EmWeb	EMWEB (SSH): Max number of SSH login sessions exceeded	A user attempted to connect via SSH when the maximum number of SSH sessions were already active.
EmWeb	Handle table overflow	All the available EmWeb connection handles are being used and the connection could not be made.
EmWeb	*ConnectionType* EmWeb socket accept() failed: errno	Socket accept failure for the specified connection type.
EmWeb	ewsNetHTTPReceive failure in NetReceiveLoop() - closing connection.	Socket receive failure.
EmWeb	EmWeb: connection allocation failed	Memory allocation failure for the new connection.
EmWeb	EMWEB TransmitPending : EWOULDBLOCK error sending data	Socket error on send.
EmWeb	ewaNetHTTPEnd: internal error - handle not in Handle table	EmWeb handle index not valid.
EmWeb	ewsNetHTTPReceive:recvBufCnt exceeds MAX_QUEUED_RECV_BUFS!	The receive buffer limit has been reached. Bad request or DoS attack.
EmWeb	EmWeb accept: XXXX	Accept function for new SSH connection failed. XXXX indicates the error info.

Table 23: CLI_UTIL Log Messages

Component	Message	Cause
CLI_UTIL	Telnet Send Failed errno = 0x%x	Failed to send text string to the telnet client.
CLI_UTIL	osapiFsDir failed	Failed to obtain the directory information from a volume's directory.

Table 24: WEB Log Messages

Component	Message	Cause
WEB	Max clients exceeded	This message is shown when the maximum allowed java client connections to the switch is exceeded.
WEB	Error on send to sockfd XXXX, closing connection	Failed to send data to the java clients through the socket.
WEB	# (XXXX) Form Submission Failed. No Action Taken.	The form submission failed and no action is taken. XXXX indicates the file under consideration.
WEB	ewaFormServe_file_download() - WEB Unknown return code from tftp download result	Unknown error returned while downloading file using TFTP from web interface.
WEB	ewaFormServe_file_upload() - Unknown return code from tftp upload result	Unknown error returned while uploading file using TFTP from web interface.
WEB	Web UI Screen with unspecified access attempted to be brought up	Failed to get application-specific authorization handle provided to EmWeb/Server by the application in ewsAuthRegister(). The specified web page will be served in read-only mode.

Table 25: CLI_WEB_MGR Log Messages

Component	Message	Cause
CLI_WEB_MGR	File size is greater than 2K	The banner file size is greater than 2K bytes.
CLI_WEB_MGR	No. of rows greater than allowed maximum of XXXX	When the number of rows exceeds the maximum allowed rows.

Table 26: SSHD Log Messages

Component	Message	Cause
SSHD	SSHD: Unable to create the global (data) semaphore	Failed to create semaphore for global data protection.
SSHD	SSHD: Msg Queue is full, event = XXXX	Failed to send the message to the SSHD message queue as message queue is full. XXXX indicates the event to be sent.
SSHD	SSHD: Unknown UI event in message, event = XXXX	Failed to dispatch the UI event to the appropriate SSHD function as it's an invalid event. XXXX indicates the event to be dispatched.
SSHD	sshdApiCnfgrCommand: Failed calling sshdIssueCmd.	Failed to send the message to the SSHD message queue.

Table 27: SSLT Log Messages

Component	Message	Cause
SSLT	SSLT: Exceeded maximum, ssltConnectionTask	Exceeded maximum allowed SSLT connections.
SSLT	SSLT: Can't connect to unsecure server at XXXX, result = YYYY, errno = ZZZZ	Failed to open connection to unsecure server. XXXX is the unsecure server socket address. YYYY is the result returned from connect function and ZZZZ is the error code.

Table 27: SSLT Log Messages

Component	Message	Cause
SSLT	SSLT: Msg Queue is full, event = XXXX	Failed to send the received message to the SSLT message queue as message queue is full. XXXX indicates the event to be sent.
SSLT	SSLT: Unknown UI event in message, event = XXXX	Failed to dispatch the received UI event to the appropriate SSLT function as it's an invalid event. XXXX indicates the event to be dispatched.
SSLT	ssltApiCnfgrCommand: Failed calling ssltIssueCmd.	Failed to send the message to the SSLT message queue.
SSLT	SSLT: Error loading certificate from file XXXX	Failed while loading the SSLcertificate from specified file. XXXX indicates the file from where the certificate is being read.
SSLT	SSLT: Error loading private key from file	Failed while loading private key for SSL connection.
SSLT	SSLT: Error setting cipher list (no valid ciphers)	Failed while setting cipher list.
SSLT	SSLT: Could not delete the SSL semaphores	Failed to delete SSL semaphores during cleanup.of all resources associated with the OpenSSL Locking semaphores.

Table 28: User_Manager Log Messages

Component	Message	Cause
User_Manager	User Login Failed for XXXX	Failed to authenticate user login. XXXX indicates the username to be authenticated.
User_Manager	Access level for user XXXX could not be determined. Setting to READ_ONLY.	Invalid access level specified for the user. The access level is set to READ_ONLY. XXXX indicates the username.
User_Manager	Could not migrate config file XXXX from version YYYY to ZZZZ. Using defaults.	Failed to migrate the config file. XXXX is the config file name. YYYY is the old version number and ZZZZ is the new version number.

SWITCHING

Table 29: Protected Ports Log Messages

Component	Message	Cause
Protected Ports	Protected Port: failed to save configuration	This appears when the protected port configuration cannot be saved.
Protected Ports	protectedPortCnfgrInitPhase1Process: Unable to create r/w lock for protectedPort	This appears when protectedPortCfgRWLock Fails.
Protected Ports	protectedPortCnfgrInitPhase2Process: Unable to register for VLAN change callback	This appears when nimRegisterIntfChange with VLAN fails.
Protected Ports	Cannot add intIfNum xxx to group yyy	This appears when an interface could not be added to a particular group.

Table 29: Protected Ports Log Messages (Cont.)

Component	Message	Cause
Protected Ports	unable to set protected port group	This appears when a dtl call fails to add interface mask at the driver level.
Protected Ports	Cannot delete intIfNum xxx from group yyy	This appears when a dtl call to delete an interface from a group fails.
Protected Ports	Cannot update group YYY after deleting interface XXX	This message appears when an update group for a interface deletion fails.
Protected Ports	Received an interface change callback while not ready to receive it	This appears when an interface change call back has come before the protected port component is ready.

Table 30: IP Subnet VLANS Log Messages

Component	Message	Cause
IPsubnet vlans	ERROR vlanIpSubnetSubnetValid :Invalid subnet	This occurs when an invalid pair of subnet and netmask has come from the CLI.
IPsubnet vlans	IP Subnet Vlans: failed to save configuration	This message appears when save configuration of subnet vlans failed.
IPsubnet vlans	vlanIpSubnetCnfgrInitPhase1Process: Unable to create r/w lock for vlanIpSubnet	This appears when a read/write lock creations fails.
IPsubnet vlans	vlanIpSubnetCnfgrInitPhase2Process: Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications.
IPsubnet vlans	vlanIpSubnetCnfgrFiniPhase1Process: could not delete avl semaphore	This appears when a semaphore deletion of this component fails.
IPsubnet vlans	vlanIpSubnetDtlVlanCreate: Failed	This appears when a dtl call fails to add an entry into the table.
IPsubnet vlans	vlanIpSubnetSubnetDeleteApply: Failed	This appears when a dtl fails to delete an entry from the table.
IPsubnet vlans	vlanIpSubnetVlanChangeCallback: Failed to add an Entry	This appears when a dtl fails to add an entry for a vlan add notify event.
IPsubnet vlans	vlanIpSubnetVlanChangeCallback: Failed to delete an Entry	This appears when a dtl fails to delete an entry for an vlan delete notify event.

Table 31: MAC-based VLANs Log Messages

Component	Message	Cause
Mac based VLANS	MAC VLANs: Failed to save configuration	This message appears when save configuration of Mac vlans failed.
Mac based VLANS	vlanMacCnfgrInitPhase1Process: Unable to create r/w lock for vlanMac	This appears when a read/write lock creations fails.
Mac based VLANS	Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications.
Mac based VLANS	vlanMacCnfgrFiniPhase1Process: could not delete avl semaphore	This appears when a semaphore deletion of this component fails.
Mac based VLANS	vlanMacAddApply: Failed to add an entry	This appears when a dtl call fails to add an entry into the table.

Table 31: MAC-based VLANs Log Messages (Cont.)

Component	Message	Cause
Mac based VLANS	vlanMacDeleteApply: Unable to delete an Entry	This appears when a dtl fails to delete an entry from the table.
Mac based VLANS	vlanMacVlanChangeCallback: Failed to add an entry	This appears when a dtl fails to add an entry for a vlan add notify event.
Mac based VLANS	vlanMacVlanChangeCallback: Failed to delete an entry	This appears when a dtl fails to delete an entry for an vlan delete notify event.

Table 32: 802.1x Log Messages

Component	Message	Cause
802.1X	*function*: Failed calling dot1xIssueCmd	802.1X message queue is full.
802.1X	*function:* EAP message not received from server	RADIUS server did not send required EAP message.
802.1X	*function*: Out of System buffers	802.1X cannot process/transmit message due to lack of internal buffers.
802.1X	*function*: could not set state to <authorized/ unauthorized>, intf xxx	DTL call failed setting authorization state of the port.
802.1X	dot1xApplyConfigData: Unable to <enable/ disable> dot1x in driver	DTL call failed enabling/disabling 802.1X.
802.1X	dot1xSendRespToServer: dot1xRadiusAccessRequestSend failed	Failed sending message to RADIUS server.
802.1X	dot1xRadiusAcceptProcess: error calling radiusAccountingStart, ifIndex = xxx	Failed sending accounting start to RADIUS server.
802.1X	*function*: failed sending terminate cause, intf xxx	Failed sending accounting stop to RADIUS server.

Table 33: IGMP Snooping Log Messages

Component	Message	Cause
IGMP Snooping	*function*: osapiMessageSend failed	IGMP Snooping message queue is full.
IGMP Snooping	Failed to set global igmp snooping mode to xxx	Failed to set global IGMP Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp snooping mode xxx for interface yyy	Failed to set interface IGMP Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp mrouter mode xxx for interface yyy	Failed to set interface multicast router mode due to IGMP Snooping message queue being full.
IGMP Snooping	Failed to set igmp snooping mode xxx for vlan yyy	Failed to set VLAN IGM Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp mrouter mode %d for interface xxx on Vlan yyy	Failed to set VLAN multicast router mode due to IGMP Snooping message queue being full.
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating small buffers	Could not allocate buffers for small IGMP packets.
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating large buffers	Could not allocate buffers for large IGMP packets.

Table 34: GARP/GVRP/GMRP Log Messages

Component	Message	Cause
GARP/GVRP/ GMRP	garpSpanState, garpIfStateChange, GarpIssueCmd, garpDot1sChangeCallBack, garpApiCnfgrCommand, garpLeaveAllTimerCallback, garpTimerCallback: QUEUE SEND FAILURE:	The garpQueue is full, logs specifics of the message content like internal interface number, type of message, etc.
GARP/GVRP/ GMRP	GarpSendPDU: QUEUE SEND FAILURE	The garpPduQueue is full, logs specific of the GPDU, internal interface number, vlan id, buffer handle, etc.
GARP/GVRP/ GMRP	garpMapIntfIsConfigurable, gmrpMapIntfIsConfigurable: Error accessing GARP/GMRP config data for interface %d in garpMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.
GARP/GVRP/ GMRP	garpTraceMsgQueueUsage: garpQueue usage has exceeded fifty/eighty/ninety percent	Traces the build up of message queue. Helpful in determining the load on GARP.
GARP/GVRP/ GMRP	gid_destroy_port: Error Removing port %d registration for vlan-mac %d - %02X:%02X:%02X:%02X:%02X:%02X	Mismatch between the gmd (gmrp database) and MFDB.
GARP/GVRP/ GMRP	gmd_create_entry**:** GMRP failure adding MFDB entry: vlan %d and address %s	MFDB table is full.

Table 35: 802.3ad Log Messages

Component	Message	Cause
802.3ad	dot3adReceiveMachine: received default event %x	Received a LAG PDU and the RX state machine is ignoring this LAGPDU.
802.3ad	dot3adNimEventCompletionCallback, dot3adNimEventCreateCompletionCallback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)	The event sent to NIM was not completed successfully.

Table 36: FDB Log Message

Component	Message	Cause
FDB	fdbSetAddressAgingTimeOut: Failure setting fid %d address aging timeout to %d	Unable to set the age time in the hardware.

Table 37: Double VLAN Tag Log Message

Component	Message	Cause
Double Vlan Tag	dvlantagIntfIsConfigurable: Error accessing dvlantag config data for interface %d	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.

Table 38: MFDB Log Message

Component	Message	Cause
MFDB	mfdbTreeEntryUpdate: entry does not exist	Trying to update a non existing entry.

Table 39: 802.1Q Log Messages

Component	Message	Cause
802.1Q	dot1qIssueCmd: Unable to send message %d to dot1qMsgQueue for vlan %d - %d msgs in queue	dot1qMsgQueue is full.
802.1Q	dot1qVlanCreateProcess: Attempt to create a vlan with an invalid vlan id %d ; VLAN %d not in range,	This accommodates for reserved vlan ids. i.e. 4094 - x.
802.1Q	dot1qMapIntfIsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.
802.1Q	dot1qVlanDeleteProcess: Deleting the default VLAN	Typically encountered during clear Vlan and clear config.
802.1Q	dot1qVlanMemberSetModify, dot1qVlanTaggedMemberSetModify: Dynamic entry %d can only be modified after it is converted to static	If this vlan is a learnt via GVRP then we cannot modify it's member set via management.

Table 40: 802.1S Log Messages

Component	Message	Cause
802.1S	dot1sIssueCmd: Dot1s Msg Queue is full!!!!Event: %u, on interface: %u, for instance: %u	The message Queue is full.
802.1S	dot1sStateMachineRxBpdu(): Rcvd BPDU Discarded	The current conditions, like port is not enabled or we are currently not finished processing another BPDU on the same interface, does not allow us to process this BPDU.
802.1S	dot1sBpduTransmit(): could not get a buffer	Out of system buffers.

Table 41: Port Mac Locking Log Message

Component	Message	Cause
Port Mac Locking	pmlMapIntfIsConfigurable: Error accessing PML config data for interface %d in pmlMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.

Table 42: Protocol-based VLANs Log Messages

Component	Message	Cause
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register NIM callback	Appears when nimRegisterIntfChange fails to register pbVlan for link state changes.

Table 42: Protocol-based VLANs Log Messages

Component	Message	Cause
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with vlans	Appears when vlanRegisterForChange fails to register pbVlan for vlan changes.
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with nvStore	Appears when nvStoreRegister fails to register save and restore functions for configuration save.

QoS

Table 43: ACL Log Messages

Component	Message	Cause
ACL	Total number of ACL rules (x) exceeds max (y) on intf i.	The combination of all ACLs applied to an interface has resulted in requiring more rules than the platform supports.
ACL	ACL *name*, rule *x*: This rule is not being logged	The ACL configuration has resulted in a requirement for more logging rules than the platform supports. The specified rule is functioning normally except for the logging action.
ACL	aclLogTask: error logging ACL rule trap for correlator *number*	The system was unable to send an SNMP trap for this ACL rule which contains a logging attribute.
ACL	IP ACL *number*: Forced truncation of one or more rules during config migration	While processing the saved configuration, the system encountered an ACL with more rules than is supported by the current version. This may happen when code is updated to a version supporting fewer rules per ACL than the previous version.

Table 44: CoS Log Message

Component	Message	Cause
COS	cosCnfgrInitPhase3Process: Unable to apply saved config -- using factory defaults	The COS component was unable to apply the saved configuration and has initialized to the factory default settings.

Table 45: DiffServ Log Messages

Component	Message	Cause
DiffServ	diffserv.c 165: diffServRestore Failed to reset DiffServ. Recommend resetting device	While attempting to clear the running configuration an error was encountered in removing the current settings. This may lead to an inconsistent state in the system and resetting is advised.
DiffServ	Policy invalid for service intf: "policy *name*, intIfNum *x*, direction *y*	The DiffServ policy definition is not compatible with the capabilities of the interface specified. Check the platform release notes for information on configuration limitations.

ROUTING

Table 46: DHCP Relay Log Messages

Component	*Message*	*Cause*
DHCP relay	REQUEST hops field more than config value	The DHCP relay agent has processed a DHCP request whose HOPS field is larger than the maximum value allowed. The relay agent will not forward a message with a hop count greater than 4.
DHCP relay	Request's seconds field less than the config value	The DHCP relay agent has processed a DHCP request whose SECS field is larger than the configured minimum wait time allowed.
DHCP relay	processDhcpPacket: invalid DHCP packet type: %u\n	The DHCP relay agent has processed an invalid DHCP packet. Such packets are discarded by the relay agent.

Table 47: Routing Table Manager Log Messages

Component	*Message*	*Cause*
Routing Table Manager	RTO is full. Routing table contains 8000 best routes, 8000 total routes.	The routing table manager, also called “RTO,” stores a limited number of best routes, based on hardware capacity. When the routing table becomes full, RTO logs this alert. The count of total routes includes alternate routes, which are not installed in hardware.
Routing Table Manager	RTO no longer full. Bad adds: 10. Routing table contains 7999 best routes, 7999 total routes.	When the number of best routes drops below full capacity, RTO logs this notice. The number of bad adds may give an indication of the number of route adds that failed while RTO was full, but a full routing table is only one reason why this count is incremented.

Table 48: VRRP Log Messages

Component	*Message*	*Cause*
VRRP	Changing priority to 255 for virtual router with VRID 1 on interface 0/1	When the router is configured with the address being used as the virtual router ID, the router’s priority is automatically set to the maximum value to ensure that the address owner becomes the VRRP master.
VRRP	Changing priority to 100 for virtual router with VRID 1 on interface 0/1	When the router is no longer the address owner, the sofware reverts the router’s priority to the default.
VRRP	vrrpPacketValidate: Invalid TTL	VRRP ignored an incoming message whose time to live (TTL) in the IP header was not 255.

Table 49: ARP Log Message

Component	Message	Cause
ARP	ARP received mapping for IP address xxx to MAC address yyy. This IP address may be configured on two stations.	When we receive an ARP response with different MAC address from another station with the same IP address as ours. This might be a case of misconfiguration.

Table 50: RIP Log Message

Component	Message	Cause
RIP	RIP : discard response from xxx via unexpected interface	When RIP response is received with a source address not matching the incoming interface's subnet.

TECHNOLOGIES

Table 51: Driver Error Messages

Component	Message	Cause
Driver	Invalid USP unit = x, slot = x, port = x	A port was not able to be translated correctly during the receive.
Driver	In hapiBroadSystemMacAddress call to 'bcm_l2_addr_add' - FAILED : x	Failed to add an L2 address to the MAC table. This should only happen when a hash collision occurs or the table is full.
Driver	Failed installing mirror action - rest of the policy applied successfully	A previously configured probe port is not being used in the policy. The release notes state that only a single probe port can be configured.
Driver	Policy x does not contain rule x	The rule was not added to the policy due to a discrepancy in the rule count for this specific policy. Additionally, the message can be displayed when an old rule is being modified, but the old rule is not in the policy.
Driver	ERROR: policy x, tmpPolicy x, size x, data x x x x x x x x	An issue installing the policy due to a possible duplicate hash.
Driver	ACL x not found in internal table	Attempting to delete a non-existent ACL.
Driver	ACL internal table overflow	Attempting to add an ACL to a full table.
Driver	In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x	Attempting to configure the bandwidth beyond it's capabilities.
Driver	USL: failed to put sync response on queue	A response to a sync request was not enqueued. This could indicate that a previous sync request was received after it was timed out.
Driver	USL: failed to sync ipmc table on unit = x	Either the transport failed or the message was dropped.
Driver	usl_task_ipmc_msg_send(): failed to send with x	Either the transport failed or the message was dropped.

Table 51: Driver Error Messages (Cont.)

Component	*Message*	*Cause*
Driver	USL: No available entries in the STG table	The Spanning Tree Group table is full in USL.
Driver	USL: failed to sync stg table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Driver	USL: A Trunk doesn't exist in USL	Attempting to modify a Trunk that doesn’t exist.
Driver	USL: A Trunk being created by bcmx already existed in USL	Possible synchronization issue between the application, hardware, and sync layer.
Driver	USL: A Trunk being destroyed doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
Driver	USL: A Trunk being set doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
Driver	USL: failed to sync trunk table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Driver	USL: Mcast entry not found on a join	Possible synchronization issue between the application, hardware, and sync layer.
Driver	USL: Mcast entry not found on a leave	Possible synchronization issue between the application, hardware, and sync layer.
Driver	USL: failed to sync dvlan data on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Driver	USL: failed to sync policy table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Driver	USL: failed to sync VLAN table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Driver	Invalid LAG id x	Possible synchronization issue between the BCM driver and HAPI.
Driver	Invalid uport calculated from the BCM uport bcmx_l2_addr->lport = x	Uport not valid from BCM driver.
Driver	Invalid USP calculated from the BCM uport\nbcmx_l2_addr->lport = x	USP not able to be calculated from the learn event for BCM driver.
Driver	Unable to insert route R/P	Route R with prefix P could not be inserted in the hardware route table. A retry will be issued.
Driver	Unable to Insert host H	Host H could not be inserted in hardware host table. A retry will be issued.
Driver	USL: failed to sync L3 Intf table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Driver	USL: failed to sync L3 Host table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Driver	USL: failed to sync L3 Route table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.

Table 51: Driver Error Messages (Cont.)

Component	Message	Cause
Driver	USL: failed to sync initiator table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Driver	USL: failed to sync terminator table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Driver	USL: failed to sync ip-multicast table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.

O/S SUPPORT

Table 52: OSAPI VxWorks Log Messages

Component	Message	Cause
OSAPI VxWorks	ftruncate failed – File resides on a read-only file system.	ftruncate is called to correctly set the file's size in the file system after a write. The file system is R/W so this msg indicates the file system may be corrupted.
OSAPI VxWorks	ftruncate failed – File is open for reading only.	ftruncate is called to correctly set the file's size in the file system after a write. The file is opened for R/W so this msg indicates the file system may be corrupted.
OSAPI VxWorks	ftruncate failed – File descriptor refers to a file on which this operation is impossible.	ftruncate is called to correctly set the file's size in the file system after a write. This msg indicates the file system may be corrupted.
OSAPI VxWorks	ftruncate failed – Returned an unknown code in errno.	ftruncate is called to correctly set the file's size in the file system after a write. This msg indicates the file system may be corrupted.
OSAPI VxWorks	ping: bad host!	The address requested to ping can not be converted to an Internet address.
OSAPI VxWorks	osapiTaskDelete: Failed for (XX) error YYY	The requested task can not be deleted because: the requested deletion is called from an ISR, the task is already deleted, or the task ID is invalid.
OSAPI VxWorks	osapiCleanupIf: NetIPGet	During the call to remove the interface from the route table, the attempt to get an ipv4 interface address from the stack failed.
OSAPI VxWorks	osapiCleanupIf: NetMaskGet	During the call to remove the interface from the route table ,the attempt to get the ipv4 interface mask from the stack failed.
OSAPI VxWorks	osapiCleanupIf: NetIpDel	During the call to remove the interface from the route table, the attempt to delete the primary ipv4 address from the stack failed.
OSAPI VxWorks	osapiSemaTake failed	The requested semaphore can not be taken because: the call is made from an ISR or the semaphore ID is invalid.

Section 11: List of Commands

