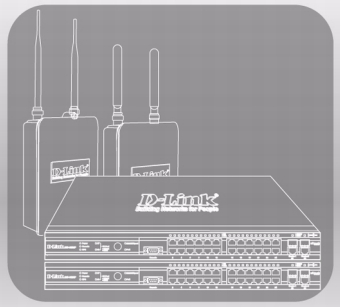
D-Link
Building Networks for People



# CLI Command Reference

Product Model : **DWS-3000 Series**
**DWL-3500AP/8500AP**

Unified Wired & Wireless Access System

Release 2.1

## REVISION HISTORY

| Revision | Date | Change Description |
|---|---|---|
| Release 2.1 | 01/31/08 | |
| | | **Added :**<br>• "dot1x guest-vlan" on page 74<br>• "dot1x guest-vlan supplicant" on page 74<br>• "tunnel-mtu" on page 145<br>• "show wireless tunnel-mtu" on page 149<br>• "station-isolation" on page 175<br>• "antenna" on page 176<br>• "Captive Portal Global Commands" on page 204<br>• "Captive Portal Configuration Commands" on page 206<br>• "Captive Portal Status Commands" on page 213<br>• "Captive Portal Client Connection Commands" on page 215<br>• "Captive Portal Interface Commands" on page 218<br>• "Captive Portal Local User Commands" on page 219<br>• "Captive Portal Activity Log Commands" on page 224<br>• "radius server attribute 4" on page 319<br>• "authorization network radius" on page 321 |
| | | **Updated:**<br>• "Command Modes" on page 30<br>• "network mgmt_vlan" on page 53<br>• "vlan" on page 53<br>• "vlan makestatic" on page 54<br>• "vlan name" on page 54<br>• "vlan participation" on page 55<br>• "vlan participation all" on page 55<br>• "vlan port pvid all" on page 56<br>• "vlan port tagging all" on page 56<br>• "vlan pvid" on page 59<br>• "vlan tagging" on page 59<br>• "show vlan" on page 60<br>• "show vlan brief" on page 61<br>• "show dot1x" on page 79<br>• "vlan routing" on page 129<br>• "show wireless ap profile radio" on page 181<br>• "show interface ethernet" on page 259 |

# Table of Contents

# List of Tables

# About This Book

This document describes command-line interface (CLI) commands you use to view and configure D-Link Unified Wired/Wireless Access System. 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.

## Document Audience

This document is for system administrators who configure and operate D-Link Unified Wired/ Wireless Access System.This document assumes that the reader has a basic knowledge of Ethernet and networking concepts.

## 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. D-Link Unified Wired/Wireless Access System provides a flexible solution to these ever-increasing needs.

D-Link Unified Wired/Wireless Access System includes a set of comprehensive management functions for managing both wired and wireless networks. You can manage the D-Link Unified Wired/Wireless Access System by using one of the following three methods:

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

Each of the D-Link Unified Wired/Wireless Access System 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.

# 1

# 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 chapter describes the CLI syntax, conventions, and modes. It contains the following sections:



## 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 CLI 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:<br>**a** (32 bits)<br>**a.b** (8.24 bits)<br>**a.b.c** (8.8.16 bits)<br>**a.b.c.d** (8.8.8.8)<br>In addition to these formats, the CLI accepts decimal, hexidecimal and octal formats through the following input formats (where *n* is any valid hexidecimal, octal or decimal number):<br>**0xn** (CLI assumes hexidecimal format)<br>**0n** (CLI assumes octal format with leading zeros)<br>**n** (CLI assumes decimal format) |
| Interface or slot/port | Valid slot and port number separated by forward slashes. For example, 0/1 represents slot 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

D-Link Unified Wired/Wireless Access System software references physical entities such as cards and ports by using a slot/port naming convention. The D-Link Unified Wired/Wireless Access System 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.<br>VLAN routing interfaces are only used for routing functions.<br>Loopback interfaces are logical interfaces that are always up.<br>Tunnel interfaces are logical point-to-point links that carry encapsulated packets. |
| CPU ports | CPU ports are handled by the driver as one or more physical entities located on physical slots. |

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

# Command Modes

The CLI groups commands into modes according to the command function. Each of the command modes supports specific D-Link Unified Wired/Wireless Access System 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 | `Switch>` | Contains a limited set of commands to view basic system information. |
| Privileged EXEC | `Switch#` | Allows you to issue any **`EXEC`** command, enter the VLAN mode, or enter the Global Configuration mode. |
| Global Config | `Switch (Config)#` | Groups general setup commands and permits you to make modifications to the running configuration. |
| VLAN Config | `Switch (Vlan)#` | Groups all the VLAN commands. |
| Interface Config | `Switch (Interface <slot/port>)#`<br>`Switch (Interface Loopback <id>)#`<br>`Switch (Interface Tunnel <id>)#` | Manages the operation of an interface and provides access to the router interface configuration commands.<br>Use this mode to set up a physical port for a specific logical connection operation. |
| Line Config | `Switch (line)#` | Contains commands to configure outbound telnet settings and console interface settings. |
| Policy Map Config | `Switch (Config-policy-map)#` | Contains the QoS Policy-Map configuration commands. |
| Policy Class Config | `Switch (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 | `Switch (Config-class-map)#` | Contains the QoS class map configuration commands.. |
| MAC Access-list Config | `Switch (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 | `Switch (Tacacs)#` | Contains commands to configure properties for the TACACS servers. |
| DHCP Pool Config | `Switch (Config dhcp-pool)#` | Contains the DHCP server IP address pool configuration commands. |

**Table 5. CLI Command Modes**

| Command Mode | Prompt | Mode Description |
|---|---|---|
| Wireless Config Mode | `Switch (Config-wireless)#` | Contains global WLAN switch configuration commands and provides access to other WLAN command modes. |
| AP Config Mode | `Switch (Config-ap)#` | Contains commands to configure entries in the local AP database, which is used for AP validation. |
| AP Profile Config Mode | `Switch (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 | `Switch (Config-ap-profile-radio)#` | Contains commands to modify the radio configuration parameters for an AP profile. |
| AP Profile VAP Config Mode | `Switch (Config-ap-profile-vap)#` | Contains commands to configure radio 1 or radio 2 within an AP profile. |
| Network Config Mode | `Switch (Config-network)#` | Contains commands to configure WLAN settings for up to 64 different networks. |
| Captive Portal Config Mode | `Switch (Config-CP)#` | Contains commands to configure global captive portal settings |
| Captive Portal Instance Mode | `Switch (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 **`interface tunnel`** *<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`***. |

**Table 6. CLI Mode Access and Exit**

| Command Mode | Access Method | Exit or Access Previous Mode |
|---|---|---|
| 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**. | 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***. |
| 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** *<0-7>*, where *<0-7>* is the VAP ID. | To exit to AP Profile Radio Config-mode, 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***. |
| Captive Portal Config Mode | From the Global Config mode, enter **captive-portal**. | To exit to the Captive Portal Config mode, enter **exit**. 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 Instance 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 |
|---|---|
| DEL 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 |

**Table 8. CLI Editing Conventions**

| Key Sequence | Description |
|---|---|
| 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 |
| 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.

```
(switch) >?

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.

```
(switch) #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.

```
(switch) #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:

```
(switch) #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 293.

# 2

# Switching Commands

This chapter describes the switching commands available in the D-Link Unified Wired/ Wireless Access System CLI.

The Switching Commands chapter includes the following sections:



**CAUTION:** The commands in this chapter 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 D-Link Unified Wired/Wireless Access System 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 124.

**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 are:

**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 are:

**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

**Interface** Valid slot and port number separated by forward slashes.

**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 93.

**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

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

**Default** 802.1s

**Format** `spanning-tree forceversion` *<802.1d | 802.1s | 802.1w>*

**Mode** Global Config

### *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 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** **spanning-tree mst priority** *<mstid>*

**Mode** Global Config

## *spanning-tree mst vlan*

This command adds an association between a multiple spanning tree instance and a VLAN so that the VLAN is 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 *<vlanid>* corresponds to an existing VLAN ID.

**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 a VLAN so that the VLAN is again be 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 *<vlanid>* corresponds to an existing VLAN ID.

**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`

**Modes** Privileged EXEC
User EXEC

**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.

**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`

**Modes** Privileged EXEC
User EXEC

**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>*

**Modes** Privileged EXEC
User EXEC

**Hello Time** Admin hello time for this port.

**Port mode** Enabled or disabled.

**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.

**RST BPDUs Transmitted** Rapid Spanning Tree Protocol Bridge Protocol Data Units sent

**RST 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

**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

**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.

**Auto-Calculate External Port Path Cost** Indicates whether auto calculation for external port path cost is enabled.

**External Port Path Cost** Configured value of the external Port Path Cost parameter.

**Designated Root** The Identifier of the designated root for this port.

**Designated Port Cost** Path Cost offered to the LAN by the Designated Port

**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.

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.

**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.

**Port Path Cost** The configured path cost for the specified interface.

**Designated Root** Identifier of the designated root for this port within the CST.

**Designated Port Cost** Path Cost offered to the LAN by the Designated 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.

**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 Port Cost** The configured path cost for this port.

## *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}*

**Modes** Privileged EXEC
User EXEC

**MST Instance ID** The MST instance associated with this port.

**Interface** Valid slot and port number separated by forward slashes.

**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.

**Link Status** The operational status of the link. Possible values are “Up” or “Down”.

**Link Trap** The link trap configuration for the specified interface.

## *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`

**Modes** Privileged EXEC
User EXEC

**MST Instance ID List** List of multiple spanning trees IDs currently configured.

**For each MSTID:**

**Associated FIDs** List of forwarding database identifiers associated with this instance.

**Associated VLANs** 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`

**Modes** Privileged EXEC
User EXEC

**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.

**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** Identifier used to identify the configuration currently being used.

**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>*

**Modes** Privileged EXEC
User EXEC

**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 <2-3965> <name>`

**Mode** VLAN Config

### *no vlan name*

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

**Format** `no vlan name <2-3965>`

**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:

**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 participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number. You can use the following participation options:

- 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.

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

**Mode** Global Config

## vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces. The modes defined as follows:

- 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.

**Default** all

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

**Mode** Global Config

### *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*.

**NOTE:** D-Link Unified Wired/Wireless Access System software supports IPv4 protocol-based VLANs.

**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.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

**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.

You should create the referenced VLAN before you create the protocol-based VLAN except when you configure GVRP to create the VLAN.

**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.

You should create the referenced VLAN before you create the protocol-based VLAN except when you configure GVRP to create the VLAN.

**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>`

**Modes** Privileged EXEC

User EXEC

**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 forward slashes. 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.

**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`

**Modes** Privileged EXEC

User EXEC

**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}*

**Modes** Privileged EXEC
User EXEC

**Interface** Valid slot and port number separated by forward slashes. 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

**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

**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}]`

**Modes** Privileged EXEC
User EXEC

**Interface** Valid slot and port number separated by forward slashes.

**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}]`

**Modes** Privileged EXEC
User EXEC

**Interface** Valid slot and port number separated by forward slashes.

**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.

# Provisioning (IEEE 802.1p) Commands

This section describes the commands you use to configure provisioning, 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>*

**Modes** Privileged EXEC
User EXEC

**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** User EXEC
Privileged EXEC

**Name** A string associated with this group as a convenience. It can be up to 32 alpha-numeric 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>*

**Modes** 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*

**Modes** 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>`

**Modes** 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`

**Modes** 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>`

**Modes** 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`

**Modes** Interface Config
Global Config

## *show garp*

This command displays GARP information.

**Format** `show garp`

**Modes** Privileged EXEC
User EXEC

**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`**

**Modes** 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`**

**Modes** 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}*

**Modes** Privileged EXEC
User EXEC

**Interface** Valid slot and port number separated by forward slashes.

**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`

**Modes** 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`

**Modes** 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}*

**Modes** Privileged EXEC
User EXEC

**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).

**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

**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. D-Link Unified Wired/Wireless Access System 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 specifies an active VLAN as an IEEE 802.1x guest VLAN. The ***<vlan-id>*** range is 1 to the maximum VLAN ID.

**Format** `dot1x guest-vlan <vlan-id>`

**Mode** Interface Config

### no dot1x guest-vlan

This command removes the specified VLAN an IEEE 802.1x guest VLAN. The ***<vlan-id>*** range is 1 to the maximum VLAN ID.

**Format** `no dot1x guest-vlan <vlan-id>`

**Mode** Interface Config

## dot1x guest-vlan supplicant

Use this command to allow 802.1x-capable supplicants to access the guest VLAN.

**Default** disabled

**Format** `dot1x guest-vlan supplicant`

**Mode** Global Config

### no dot1x guest-vlan supplicant

Use this command to prohibit 802.1x-capable supplicants from accessing the guest VLAN.

**Format** `no dot1x guest-vlan supplicant`

**Mode** Global 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'. If the control mode is not 'auto' 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 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.

**Default** auto

**Format** **dot1x port-control** *{force-unauthorized | force-authorized | auto}*

**Mode** Interface Config

### *no dot1x port-control*

This command sets the authentication 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.

**Default** auto

**Format** `dot1x port-control all` *{force-unauthorized | force-authorized | auto}*

**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'. If the control mode is not 'auto' an error will be returned.

**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:

- **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** reauth-period: 3600 seconds
quiet-period: 60 seconds
tx-period: 30 seconds
supp-timeout: 30 seconds
server-timeout: 30 seconds

**Format** `dot1x timeout` *{{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** *{reauth-period | quiet-period | tx-period | supp-timeout | server-timeout}*

**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

**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

**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 any of the optional parameters, the global dot1x configuration summary is displayed.

**Administrative mode** Indicates whether authentication control on the switch is enabled or disabled.

**Supplicant Allowed in Guest VLAN** Indicates whether the Guest VLAN for supplicants feature is enabled or disabled.

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

```
(DWS-3026) #show dot1x

Administrative Mode.............. Disabled
Supplicant Allowed In Guest Vlan.. Disabled
```

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

**Port** The interface whose configuration is displayed.

**Control Mode** The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto.

**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.

**Key Transmission Enabled** Indicates if the key is transmitted to the supplicant for the specified port.

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

**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.

**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.

**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 ID of the VLAN used for unauthenticated or authentication failed users.

**Guest VLAN Period** The value, in seconds, of the timer used by the Guest VLAN Authentication. The guest VLAN timeout must be a value in the range of 1 and 300. The default value is 90. The guest VLAN becomes operational after this timeout is reached giving enough time to the user to get authenticated.

**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 ID assigned by the RADIUS server.

**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.

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

```
(DWS-3026) #show dot1x detail 0/1

Port..................................... 0/1
Protocol Version......................... 1
PAE Capabilities......................... Authenticator
Authenticator PAE State.................. Initialize
Backend Authentication State............. Initialize
Quiet Period............................. 60
Transmit Period.......................... 30
Guest VLAN ID............................ 0
Guest Vlan Period........................ 90
Supplicant Timeout....................... 30
Server Timeout (secs).................... 30
Maximum Requests......................... 2
Vlan Assigned............................ 0
Reauthentication Period.................. 3600
Reauthentication Enabled................. FALSE
Key Transmission Enabled................. FALSE
Control Direction........................ both
```

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

**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.

**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 users*

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

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

**Mode** Privileged EXEC

**User** 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

**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.

## Storm-Control Commands

This section describes commands you use to configure storm control and view storm-control configuration information. 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. The Storm Control feature can help maintain network performance.

## 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** 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** Interface Config

## storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold in terms of percentage of the interface speed for an interface. When you use this command, broadcast storm recovery mode is enabled on the interface and broadcast storm recovery is active. 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 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 in terms of percentage of the interface speed 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.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 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 in terms of percentage of the interface speed for an interface 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`

**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, in terms of percentage of the interface speed, for all interfaces 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 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 in terms of percentage of the interface speed for an interface, 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 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 in terms of percentage of the interface speed for an interface, and enables unicast storm recovery 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** 5

**Format** `storm-control unicast all level <0-100>`

**Mode** Global Config

### *no storm-control unicast all level*

This command returns 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 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. 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

**Bcast Mode** Shows whether the broadcast storm control mode is enabled or 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.

# Port-Channel/LAG (802.3ad) Commands

This section describes the commands you use to configure port-channels, which 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 40.

**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 40.

**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 273

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

**Mode** Global 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

### 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 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

## 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**

**Modes** Privileged EXEC
User EXEC

For each port-channel the following information is displayed:

**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.

**Type** Shows whether the port-channel is statically or dynamically maintained.

**LACP Device Type/Timeout** The timeout (**long** or **short**) for the type of device (**actor** or **partner**)

**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}*

**Modes** Privileged EXEC
User EXEC

**Logical Interface** Valid slot and port number separated by forward slashes.

**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.

**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.

**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.

**Active Ports** This field lists ports that are actively participating in the port-channel (LAG).

# 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 D-Link Unified Wired/Wireless Access System 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

**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.

## *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. You can create up to 100 static MAC filters.

**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 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

**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).

## 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

**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.

**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:).

# IGMP Snooping Configuration Commands

This section describes the commands you use to configure IGMP snooping. D-Link Unified Wired/Wireless Access System 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`

**Modes** 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`

**Modes** 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`

**Modes** 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>*

**Modes** Interface Config
Global Config

**Format** **set igmp groupmembership-interval** *<vlan_id> <2-3600>*

**Modes** 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**

**Modes** 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 3599 seconds.

**Default** 10 seconds

**Format** **set igmp maxresponse** *<1-3599>*

**Modes** Global Config
Interface Config

**Format** **set igmp maxresponse** *<vlan_id> <1-3599>*

**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**

**Modes** 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>`

**Modes** 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`

**Modes** 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:

**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:

**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:

**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

**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

**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

**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:).

# 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 312.

## *port-security*

This command enables port locking at the system level (Global Config) or port level (Interface Config)

**Default** disabled

**Format** `port-security`

**Modes** 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`

**Modes** 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

**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:

**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

**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

**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

**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 Configuration

### no lldp receive

Use this command to return the reception of LLDPDUs to the default value.

**Format** `lldp receive`

**Mode** Interface Configuration

## 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 See "snmp-server" on page 310. 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 38.

**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.

**Format** `clear lldp statistics`

**Mode** Privileged Exec

## clear lldp remote-data

Use this command to delete all information from the LLDP remote data table.

**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

**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. |
| **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 |
| **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:

| | |
|---|---|
| **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

**Local Interface** The interface that received the LLDPDU from the remote device.

**Chassis ID** The ID of the remote device.

**Port ID** The port number that transmitted the LLDPDU.

**System Name** The system name of the remote device.

## 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

**Local Interface** The interface that received the LLDPDU from the remote device.

**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.

**Time To Live** The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

## 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

**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

**Interface** The interface that sends the LLDPDU.

**Chassis ID Subtype** The type of identification used in the Chassis ID field.

**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.

# Denial of Service Protection Commands

**NOTE:** Denial of Service (DataPlane) is not supported on the XGSII Tucana Platform. DoS is supported on XGSIII platforms only.

This section describes the commands you use to configure Denial of Service (DoS) Control. D-Link Unified Wired/Wireless Access System software provides support for classifying and blocking specific types of Denial of Service attacks. You can configure your system to monitor and block six 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 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 storm-control broadcast all`

**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

### show dos-control

This command displays Denial of Service configuration information.

**Format** `show dos-control`

**Mod** Privileged EXEC

**SIPDIP Mode** May be enabled or disabled. The factory default is disabled.

**First Fragment Mode** May be enabled or disabled. The factory default is disabled.

**Min TCP Hdr Size <0-255>** The factory default is 20.

**TCP Fragment Mode** May be enabled or disabled. The factory default is disabled.

**TCP Flag Mode** May be enabled or disabled. The factory default is disabled.

**L4 Port Mode** May be enabled or disabled. The factory default is disabled.

**ICMP Mode** May be enabled or disabled. The factory default is disabled.

**Max ICMP Pkt Size <0-1023>** The factory default is 512.

## 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

**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

**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.

**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

**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.

# 3

# Routing Commands

This chapter describes the routing commands available in the D-Link Unified Wired/Wireless Access System CLI.

The Routing Commands chapter contains the following sections:



The commands in this chapter are in one of three functional groups:

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

## Address Resolution Protocol (ARP) Commands

This section describes the commands you use to configure 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** enabled

**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

## 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

**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.**

**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

**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.

**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

**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 IPv4 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. The value for *<subnetmask>* is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface.

**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. 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>][<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>}]*

**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. D-Link Unified Wired/Wireless Access System 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 39.) 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.

**Format** **show ip brief**

**Modes** Privileged EXEC
User EXEC

**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.

**IP Forwarding Mode** Shows whether forwarding of IP frames is enabled or disabled. This is a configured value.

**Maximum Next Hops** The maximum number of next hops the packet can travel.

## show ip interface

This command displays all pertinent information about the IP interface.

**Format** `show ip interface <slot/port>`

**Modes** Privileged EXEC
User EXEC

**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.

**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.

**Routing Configuration** Displays whether Routing Configuration is enabled or disabled on the system.

**Interface Configuration Status** Displays whether the Interface Configuration is enabled or disabled on the system.

**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.

*Example: show ip interface*

```
(r2) #show ip interface 0/2

Routing Configuration.......................... Enable
Interface Configuration Status................. Enable
Forward Net Directed Broadcasts................ Disable
Proxy ARP...................................... Enable
Local Proxy ARP................................ Disable
Active State................................... Active
Link Speed Data Rate........................... 100 Full
MAC Address.................................... 00:10:4B:D2:17:83
Encapsulation Type............................. Ethernet
IP MTU......................................... 1500
```

## 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

**Interface** Valid slot and port number separated by forward slashes.

**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*, *static*, or *bgp*. 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}]*

**Mode** Privileged EXEC
User EXEC

**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, Interface
```

The columns for the routing table display the following information:

**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

**Interface** The outgoing router interface to use when forwarding traffic to the next destination

## 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]*

**Mode** Privileged EXEC
User EXEC

**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.

**BGP Routes** Total number of routes installed by BGP protocol.

**OSPF Routes** Total number of routes installed by OSPF protocol.

**Total Routes** Total number of routes in the routing table.

## 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

**Local** The local route preference value.

**Static** The static route preference value.

**OSPF Intra** The OSPF Intra route preference value.

**OSPF Inter** The OSPF Inter route preference value.

**OSPF Ext T1** The OSPF External Type-1 route preference value.

**OSPF Ext T2** The OSPF External Type-2 route preference value.

**OSPF NSSA T1** The OSPF NSSA Type-1 route preference value.

**OSPF NSSA T2** The OSPF NSSA Type-2 route preference value.

**RIP** The RIP route preference value.

**BGP4** The BGP-4 route preference value.

**NOTE:** The configuration of NSSA preferences is not supported in this release.

### *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

# 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

**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

## 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

**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

**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.

**Format** `show ip vrrp interface` *<slot/port> <vrid>*

**Modes** Privileged EXEC
User EXEC

**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.

**Advertisement interval** The advertisement interval 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.

### *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

**Interface** Valid slot and port number separated by forward slashes.

**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

## bootpdhcprelay serverip

This command configures the server IP address for BootP/DHCP Relay on the system. The *<ipaddr>* parameter is an IP address in a 4-digit dotted decimal format.

**Default** 0.0.0.0

**Format** `bootpdhcprelay serverip <ipaddr>`

**Mode** Global Config

### *no bootpdhcprelay serverip*

This command configures the default server IP address for BootP/DHCP Relay on the system.

**Format** `no bootpdhcprelay serverip`

**Mode** Global Config

## *show bootpdhcprelay*

This command displays the BootP/DHCP Relay information.

**Format** `show bootpdhcprelay`

**Modes** Privileged EXEC
User EXEC

**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.

# 4

# Wireless Commands

This chapter 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 chapter contains the following sections:



The commands in this chapter 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

**code** This parameter must identify a valid country code.

### *no country-code*

The `no` version of this command returns the configured country code to the default.

**Format** `no country-code`

**Mode** Wireless Config

## 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

**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

**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

**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

**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

**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

## *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

**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.

### *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*} *<0-168>*

**Mode** Wireless Config

**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.

**rf-scan** Time in hours to maintain an entry obtained from an RF scan.

**0-168** 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* | *client-roam* | *rf-scan*}

**Mode** Wireless Config

## *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

**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*

Use this command to set the Tunnel MTU value.

**Format** **tunnel-mtu** {*1500* | *1520*}

**Mode** Wireless Config

**1500** Set the Tunnel MTU value to 1500 bytes.

**1520** Set the Tunnel MTU value to 1520 bytes.

***Example:*** The following shows an example of the command.

```
(DWS-3024) #configure

(DWS-3024) (Config)#wireless

(DWS-3024) (Config-wireless)#tunnel-mtu ?

1500                    Set the Tunnel MTU value to 1500 bytes.
1520                    Set the Tunnel MTU value to 1520 bytes.
```

## *show wireless*

This **show** command displays the configured Unified Switch global parameters and the operational status.

**Format** **show wireless**

**Mode** Privileged EXEC
User EXEC

**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 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.

**Country Code** Shows the country in which the WLAN is operating.

**Peer Group ID** Shows the Peer group ID.

## show wireless country-code

This **show** command displays the country codes configurable on the Unified Switch.

**Format** `show wireless country-code`

**Mode** Privileged EXEC

**Code** Shows the 2-letter country code.

**Country** Shows the name of the country associated with the code.

## show wireless country-code channels

This **show** command displays the channels that can be configured for different physical radio modes for the configured country code and regulatory domain.

**Format** `show wireless country-code channels`

**Mode** Privileged EXEC

**Channel** Lists the available RF channel.

**Mode** Shows which mode is allowed for the corresponding channel. Possible values are:
B—802.11b
G—802.11g
Atheros—Atheros 2.4 GHz or 5 GHz modes (including Dynamic)
A—802.11A

## show wireless discovery

This **show** command displays the configured Unified Switch discovery methods.

**Format** `show wireless discovery`

**Mode** Privileged EXEC

**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

## 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

**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*.

## 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

**VLAN** Shows the ID and name of each VLAN in the L2 Discovery list.

## show wireless status

This **show** command displays the configured global Unified Switch status parameters.

**Format** `show wireless status`

**Mode** Privileged EXEC

**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).

**Total Clients** 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.

**Associated Clients** Total number of clients in the database. This total includes clients with an "Associated", "Authenticated", or "Disassociated" status.

**Peer Switches** Total number of peer Unified Switches detected on 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.

**WLAN Utilization** Total network utilization across all APs managed by this switch, this is an average of the global statistics received from each AP.

## show wireless statistics

This **show** command displays the current global Unified Switch statistics.

**Format** `show wireless statistics`

**Mode** Privileged EXEC

**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.

## show wireless trapflags

This **show** command displays the configured Unified Switch SNMP trap modes.

**Format** `show wireless trapflags`

**Mode** Privileged EXEC

**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.

**RF Scan Traps** Shows whether RF Scan Traps are enabled.

**Rogue AP Traps** Shows whether Rogue AP Traps are enabled.

**Wireless Status Traps** Shows whether Wireless Status Traps are enabled.

## show trapflags (modified command)

The existing D-Link Unified Wired/Wireless Access System **show trapflags** command is modified to show the global Unified Switch trap configuration. See the command "snmp-server enable traps wireless" on page 143.

## show wireless agetime

This **show** command displays the configured age times for the status database entries.

**Format** `show wireless agetime`

**Mode** Privileged EXEC

**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.

**Client Failure Status Age (hours)** Shows how long to continue to display a failed client 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.

### *show wireless tunnel-mtu*

Use this command to show the Tunnel MTU value. The value is expressed in bytes.

**Format** `show wireless tunnel-mtu`

**Mode** Privileged EXEC

***Example:*** show wireless tunnel-mtu

```
(DWS-3024) #show wireless tunnel-mtu

tunnel-mtu..................................... 1500
```

### *clear wireless statistics*

This **clear** command resets the global Unified Switch statistics.

**Format** `clear wireless statistics`

**Mode** Privileged EXEC

## 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 and 802.11b/g 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`** {*a* | *bg*} **`mode`** {*interval* | *manual* | *time*}

**Mode** Wireless Config

**a** Configure channel plan mode for 802.11a.

| | |
|---|---|
| **bg** | Configure channel plan mode for 802.11b/g. |
| **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 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** {a \| bg} **interval** *<6-24>* |
| **Mode** | Wireless Config |

| | |
|---|---|
| **a** | Configure channel plan mode for 802.11a. |
| **bg** | Configure channel plan mode for 802.11b/g. |
| **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** {a \| bg} **interval** |
| **Mode** | Wireless Config |

## channel-plan time

This command configures the channel plan time for each 802.11a and 802.11b/g 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** {a \| bg} **time** *<hh:mm>* |
| **Mode** | Wireless Config |
| **a** | Configure channel plan mode for 802.11a. |
| **bg** | Configure channel plan mode for 802.11b/g. |
| **hh:mm** | The channel plan time in 24 hour time. |

### no channel-plan time

The **no** version of this command returns the configured channel plan time to the default.

| | |
|---|---|
| **Format** | **no channel-plan** {a \| bg} **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 and 802.11b/g 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** {a | bg} **history-depth** *<0-10>*

**Mode** Wireless Config

**a** Configure channel plan mode for 802.11a.

**bg** Configure channel plan mode for 802.11b/g.

**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** {a | bg} **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

**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

**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 802.11a and 802.11b/g frequency band.

**Format** **wireless channel-plan** {a | bg} {*apply* | *clear* | *start*}

**Mode** Privileged EXEC

**a** Configure channel plan mode for 802.11a.

**bg** Configure channel plan mode for 802.11b/g.

**start** Compute a new proposed channel plan.

**clear** Clear the current proposed channel plan.

**apply** Apply the entire proposed channel plan.

## *wireless power-plan*

This command allows you to manage manual power adjustments for the managed APs.

**Format** **wireless power-plan** {*apply* | *clear* | *start*}

**Mode** Privileged EXEC

**start** Compute new proposed power adjustments.

**clear** Clear the proposed power adjustments.

**apply** Apply the 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** {a | bg}

**Mode** Privileged EXEC

**a** Configure channel plan mode for 802.11a.

**bg** Configure channel plan mode for 802.11b/g.

**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.

**Format** `show wireless channel-plan history {a | bg}`

**Mode** Privileged EXEC

**a** Configure channel plan mode for 802.11a.

**bg** Configure channel plan mode for 802.11b/g.

**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.

## *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.

**Format** `show wireless channel-plan proposed {a | bg}`

**Mode** Privileged EXEC

**a** Configure channel plan mode for 802.11a.

**bg** Configure channel plan mode for 802.11b/g.

**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.

### *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

**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.

**Format** `show wireless power-plan proposed`

**Mode** Privileged EXEC

**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.

## 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

**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 switch software on the peer switch.

**Protocol Version** Protocol version of switch software on the peer switch.

**Discovery Reason** Method for peer switch discovery.

**Age** Time since last update was received from the switch.

# 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

**macaddr** MAC address of a physical AP.

#### *no ap database*

The **no** version of this command deletes the AP from the local 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 | ack-rogue}*

**Mode** AP Config

**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.

**ack-rogue** AP is known on the network and should not be reported as rogue by the Unified Switch.

## location

This command configures a descriptive string for the AP location.

**Format** **location** *<value>*

**Mode** AP Config

**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

## 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 WS Managed.

**Default** 1 - Default

**Format** **profile** *<1-16>*

**Mode** AP Config

**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

**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.

## 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

**macaddr** The MAC Address corresponding to the AP's Ethernet interface.

**Location** A description for the AP, often based on its location.

**AP Mode** Indicates whether the AP is managed by the switch, by an administrator, or is an acknowledged Rogue on the network.

**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.

# 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 1-8 are created by default.

**Format** **network** *<1-64>*

**Mode** Wireless Config

**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 eight default networks can never be deleted.

**Format** **no network** *<1-64>*

**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

**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

**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

## 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

| | |
|---|---|
| **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 |

| | |
|---|---|
| **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 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 |

| | |
|---|---|
| **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

## *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

**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 use-ap-profile*

This command indicates to use the global AP profile RADIUS configuration for authentication on this network.

**Default** Enable

**Format** **radius use-ap-profile**

**Mode** Network Config

### *no radius use-ap-profile*

The **no** version of this command indicates to override the global AP profile RADIUS configuration with the network RADIUS parameters.

**Format** **no radius use-ap-profile**

**Mode** Network Config

## *radius server host*

This command configures the RADIUS server IP address for network authentication. The *<ipaddr>* variable is the IP Address of the RADIUS server.

**Format** **radius server host** *<ipaddr>*

**Mode** Network Config

### *no radius server host*

The **no** version of this command deletes the configured RADIUS authentication server IP address.

**Format** no radius server host

**Mode** Network Config

## *radius server secret*

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

## *radius accounting*

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 version** {wpa [wpa2] | wpa2}

**Mode** Network Config

**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

**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

**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

## *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 timeout*

This command configures the WPA2 pre-authentication timeout for the network. This specifies a timeout after which an AP can delete a pre-authentication that has not been used by the client.

**Default** 0, no timeout

**Format** `wpa2 pre-authentication timeout <0-1440>`

**Mode** Network Config

**0-1440** The WPA2 pre-authentication timeout in minutes, where *0* indicates pre-authentications do not timeout on the AP.

### *no wpa2 pre-authentication timeout*

The **no** version of this command sets the WPA2 pre-authentication timeout to its default value.

**Format** `no wpa2 pre-authentication timeout`

**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

**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

**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

## 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

**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 *D-Link Unified Wired/Wireless Access System WLAN Switching 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 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

**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 | 152}*

**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

## *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

**SSID** Service Set Identifier

**Default VLAN** Default VLAN for the network.

**Hide SSID Mode** Indicates if SSID inclusion is suppressed from the beacons.

**Security Mode** Indicates the authentication and encryption mode.

**L3 Tunnel Mode** If tunneling feature is enabled, indicates if L3 roaming is enabled on the network.

**L3 Tunnel Subnet** 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.

**WPA Versions Supported** 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.

**MAC Authentication Mode** The client MAC address authentication mode.

**RADIUS use AP Profile** Indicates if the AP profile RADIUS configuration or network RADIUS configuration is used for authentication.

**RADIUS Server IP** IP Address of RADIUS server for authentication.

**RADIUS Server Secret Configured** Indicates whether a value is configured for the RADIUS secret.

**RADIUS Accounting Mode** Indicates whether RADIUS accounting is enabled

**WEP Transfer Key Index** If WEP – Shared Key security mode is enabled, indicates which WEP key will be used for encryption.

**WEP Key Type** If WEP – Shared Key security mode is enabled, specifies the type of the WEP keys configured.

**WEP Key Length** If WEP – Shared Key security mode is enabled, specifies number of bits for the WEP Keys.

**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.

**WPA Key Type** Specifies the type of the WPA key configured (ASCII only).

**WPA Key** Indicates the pre-shared secret for WPA clients.

**WPA2 Pre-Authentication Mode** If WPA2 encryption 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 Pre-Authentication Timeout** If WPA2 pre-authentication is enabled, specifies a timeout in minutes after which an AP can delete a pre-authentication that has not been used by the client.

**WPA2 Key Forwarding Mode** If WPA2 encryption is enabled, indicates Dynamic Key Forwarding support for roaming WPA2 clients.

**WPA2 Key Caching Holdtime** Length of time a PMK will be cached by an AP after the client using this PMK has roamed away from this AP.

# 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

**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

**1-16** Identifier for the AP Profile

## *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

**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

## *radius server host*

This command configures a RADIUS server IP address global to the AP profile; it can be overridden within a VAP via the network configuration.

**Format** **radius server host** *<ipaddr>*

**Mode** AP Profile Config

**ipaddr** IP Address of the RADIUS server.

### *no radius server host*

The **no** version of this command deletes the configured RADIUS server IP address.

**Format** **no radius server host**

**Mode** AP Profile Config

## *radius server secret*

This command configures a RADIUS server secret global to the AP profile. This is an alphanumeric string in the range 0-64 characters. The secret can be overridden within each VAP via the network configuration.

**Default** None

**Format** **radius server secret**

**Mode** AP Profile Config

## *radius accounting*

This command enables RADIUS accounting mode global to the AP profile. It can be overridden within each VAP via the network configuration.

**Default** Disable

**Format** **radius accounting**

**Mode** AP Profile Config

### *no radius accounting*

The **no** version of this command disables RADIUS accounting mode global to the AP profile.

**Format** no radius accounting

**Mode** AP Profile Config

## mac authentication action

This command configures the client MAC authentication action for the AP profile. The action indicates what action to take on MAC addresses configured in the MAC authentication list, i.e. if the default action is *deny* all configured MAC addresses will be denied access. The action is applied to the MAC authentication list configured either locally or on the RADIUS server.

**Default** Allow

**Format** **mac authentication action** {*allow* | *deny*}

**Mode** AP Profile Config

**allow** Default action is allow, client MACs in the list are allowed.

**deny** Default action is deny, client MACs in the list are denied.

## mac authentication client

This command configures a client MAC address in the MAC authentication list.

**Format** **mac authentication client** *<macaddr>*

**Mode** AP Profile Config

**macaddr** A valid MAC address.

### no mac authentication client

The **no** version of this command deletes an entry from the MAC authentication list.

**Format** **no mac authentication client** *<macaddr>*

**Mode** AP Profile Config

## 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

**1-16** Source AP Profile ID

**1-16** Destination AP Profile ID

## 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

**1-16** AP Profile ID

## 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

## 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. You can also enter the `mac-authentication-client` keywords to display the configured MAC authentication list for that profile.

**Format** `show wireless ap profile` *`[<1-16> [mac-authentication-client [<macaddr>]]]`*

**Mode** Privileged EXEC

**macaddr** MAC address of a physical AP

**AP Profile ID** Existing AP profile ID

**Profile Name** A descriptive name for the corresponding AP profile ID

**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.

**RADIUS Server IP Address** The global RADIUS server IP Address for the AP profile.

**RADIUS Server Secret Configured** Indicates if the global RADIUS server secret is configured for this AP profile.

**RADIUS Accounting Mode** Indicates if the global RADIUS accounting mode is enabled or disabled for the AP Profile.

**MAC Authentication Action** Indicates the MAC authentication action, allow or deny.

**Client MAC Address** Ethernet address for a client.

# 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

**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

## *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 it operational channel.

**Default** Enabled
interval, 60 seconds

**Format** **rf-scan other-channels** [**interval** *<30-120>*]

**Mode** AP Profile Radio Config

**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

**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

**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

Use this command to enable Station Isolation. When Station Isolation is enabled, the AP blocks communication between wireless stations. The AP still allows data traffic between its wireless clients and wired devices on the network, but not among wireless clients. The Station Isolation setting is part of the configuration profile that the switch sends to the Managed AP.

**Default** disabled

**Format** `station-isolation`

**Mode** AP Profile Radio Config

### no station-isolation

Use this command to disable Station Isolation.

**Format** `station-isolation`

**Mode** AP Profile Radio Config

## super-a

This command enables the Super A mode on the radio. Super A mode enables Atheros frame compression and fast-frames mode. In order to use channel aggregation, the radio must be set to Atheros Dynamic Turbo mode.

**Default** Disabled

**Format** `super-a`

**Mode** AP Profile Radio Config

### no super-a

The `no` version of this command disables the Super A mode on the radio.

**Format** `no super-a`

**Mode** AP Profile Radio Config

## super-g

This command enables the Super G mode on the radio. Super G mode enables Atheros frame compression and fast-frames mode. In order to use channel aggregation, the radio must be set to Atheros Dynamic Turbo modes.

**Default** Disabled

**Format** `super-g`

**Mode** AP Profile Radio Config

### no super-g

The `no` version of this command disables the Super G mode on the radio.

**Format** `no super-g`

**Mode** AP Profile Radio Config

## antenna

Use this command to configure antenna diversity on the AP. If the AP has two antenna connectors, antenna diversity may be used. This can improve performance of the AP because the best antenna is selected for receive and transmit. However, if there is only one antenna, then disabling antenna diversity is recommended. Antenna diversity is disabled by default and antenna 1 (primary antenna) is selected for transmit/receive. This switch CLI command allows disabling or enabling the antenna diversity in a configuration profile for a radio of the managed AP.

You can select one of the following antenna modes:

- auto—Set Antenna Diversity mode to auto.
- primary—Select primary antenna for transmit/receive.
- secondary—Select primary antenna for transmit/receive.

**Default** primary

**Format** `antenna {auto | primary | secondary}`

**Mode** AP Profile Radio Config

### no antenna

Use this command to set the Antenna Diversity feature on the AP to the default value.

**Format** `no antenna`

**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

**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

**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

**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

**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** 256

**Format** **max-clients** *<0-256>*

**Mode** AP Profile Radio Config

**0-256** 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. If the optional parameter is specified, selection for the 802.11a channels is limited to a pre-defined subset of channels; this only applies to a radio in 802.11a mode.

**Default** Disabled

**Format** **channel auto** *[limit-a-channels]*

**Mode** AP Profile Radio Config

### no channel auto

The **no** version of this command without any parameters disables auto channel adjustment for the radio. If the optional parameter is specified, it only disables limiting the selection of the 802.11a channels.

**Format** **no channel auto** *[limit-a-channels]*

**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

**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 advertised client data rates for the radio. The supported rates are those the AP will allow when setting up communications with client stations. The advertised rates are those the AP will advertise to clients in its beacons.

**Default** 802.11a supported: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11a advertised: 6, 12, 24 Mbps
802.11b supported: 1, 2, 5.5, 11 Mbps
802.11b advertised: 1, 2 Mbps
802.11g supported: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
802.11g advertised: 1, 2, 5.5, 11 Mbps
Atheros (all modes) supported: 12, 18, 24, 36, 48, 72, 96, 108 Mbps
Atheros (all modes) advertised: 12, 24, 48 Mbps

**Format** **rate {*advertised* | *supported*}** *<value>*

**Mode** AP Profile Radio Config

**value** A valid data rate in Mbps based on radio mode.

### *no rate*

The **no** version of this command is used to remove an advertised or supported data rate from the corresponding list.

**Format** **no rate {*advertised* | *supported*}** *<value>*

**Mode** AP Profile Radio Config

**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

**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

## 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}]]]`

**Mode** Privileged EXEC

**AP Profile ID** AP profile ID.

**Profile Name** Descriptive name associated with the AP Profile ID.

**Radio Index** 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.

**Super A or Super G** Indicates if Super A/G is enabled on the radio. This can provide better performance by increasing throughput for the radio mode.

**Antenna** Shows which antenna the radio uses to send and receive, which might be primary, secondary, or auto.

**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 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.

**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.

**802.11a Limit Channel Selection** Indicates if the auto channel algorithm will limit the 802.11a channel selection to a pre-defined set of values. This value is only displayed for 802.11a mode.

**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.

**Default 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.

**Supported Rates** Indicates what data rates the AP will support in setting up communications with client stations.

**Advertised Rates** Indicates what data rates the AP will advertise to clients in its beacons.

**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 Station Isolation is enabled. When Station Isolation is enabled, the AP blocks communication between wireless stations.

## *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 | b | g | prime-a | prime-g | turbo-a | turbo-g}*

**Mode** Privileged EXEC

**Mode** Indicates the physical layer technology to use on the radio.

**Valid Rates** Indicates data rates valid for the physical mode.

# 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-duration <0-999900>}
```

**Mode** AP Profile Radio Config

| | |
|---|---|
| **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-length}**

**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

**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

**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.

# 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 <0-7>`

**Mode** AP Profile Radio Config

**0-7** 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 1-7 - 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 1-8 are applied to VAP0 – VAP7 in order.

**Format** `network <1-64>`

**Mode** AP Profile VAP Config

**1-64** A configured network ID.

## Switch 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 Switch 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

**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

**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

This command sets a TFTP path for the AP system image and optionally modifies 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; the optional parameter modifies the group size.

**Default** None, 10

**Format** `wireless ap download <url> [group-size <1-48>]`

**Mode** Privileged EXEC

**url** TFTP file path for an AP system image.

## wireless ap download start

This command initiates the AP image download process. The switch will send a request to one or all managed APs to download a new system image based on the configured TFTP URL.

**Format** `wireless ap download start [<macaddr>]`

**Mode** Privileged EXEC

**macaddr** Managed AP MAC Address.

## 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> <0-100>`

**Mode** Privileged EXEC

**macaddr** Managed AP MAC Address

**1-2** Radio Index to be configured on the managed AP

**0-100** 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

**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

**macaddr** Managed AP MAC Address

## 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

## show wireless ap status

This command displays operational status for a switch 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.

**Format** `show wireless ap [<macaddr>] status`

**Mode** Privileged EXEC

**macaddr** Switch managed AP MAC address.

**MAC Address** The Ethernet address of the switch managed AP.

**IP Address** The network IP address of the 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).

**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.

**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.

**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.

**Status** The current managed state of the AP. The possible values are:

Discovered - The AP is discovered and 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.

**Code Download Status** This indicates the current status of a code download request for this AP.

**Client Associations** Total number of clients currently associated to the AP. This is the sum of all associated 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.

## *show wireless ap radio status*

This command displays operational status for a switch 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

**macaddr** Switch managed AP MAC address.

**1-2** The radio interface on the AP.

**MAC Address** The Ethernet address of the switch 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.

**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.

**Eligible Channel List** 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.

## *show wireless ap radio channel status*

This command displays the manual channel adjustment status for a radio on a switch 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

**macaddr** switch 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.

## show wireless ap radio power status

This command displays the manual power adjustment status for a radio on a switch 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

**macaddr** Switch 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 switch 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 [<0-7>] status`

**Mode** Privileged EXEC

**macaddr** Switch managed AP MAC address

**1-2** The radio interface on the AP

**0-7** VAP ID

**MAC Address** The Ethernet address of the switch 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 Assoc** Indicates the total number of clients currently associated to the VAP.

## 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

**macaddr** Switch managed AP MAC address.

**1-2** The radio interface on the AP.

**MAC Address** The Ethernet address of the switch 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.

**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:

WS Managed - The neighbor AP is managed by this switch. The neighbor AP status can be referenced using its base MAC address.

Peer WS Managed - The neighbor AP is managed by another switch within the peer group.

Standalone - The AP is managed in standalone mode and configured as a valid AP entry (local or RADIUS).

Acknowledged Rogue - The AP is configured as a valid AP entry (local or RADIUS), it has been acknowledged and is not reported as Rogue.

Ad Hoc Rogue - The AP neighbor was detected participating in an ad hoc network.

**Age** Indicates the time since this AP was last reported from an RF scan on the radio.

## *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

**macaddr** Switch managed AP MAC address.

**1-2** The radio interface on the AP.

**MAC Address** The Ethernet address of the switch 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.

**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 values may be displayed.

RF Scan - 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 - The managed AP received a probe request from the client.

Associated - This neighbor is associated to another managed AP.

Associated to this AP - The client is associated to this managed AP on the displayed radio.

Ad Hoc Rogue - 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.

## *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

**macaddr** Managed AP MAC address.

**MAC Address** The Ethernet address of the switch 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.

**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.

**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.

## *show wireless ap radio statistics*

This command displays statistics for each physical radio on a switch 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

**macaddr** Switch managed AP MAC address.

**1-2** The radio interface on the AP.

**MAC Address** The Ethernet address of the switch 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.

**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.

**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.

## *show wireless ap radio vap statistics*

This command displays statistics for each VAP on a switch 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

**macaddr** Switch managed AP MAC address

**1-2** The radio interface on the AP

**0-7** VAP ID

**MAC Address** The Ethernet address of the switch 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.

**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.

**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.

## *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

**File Name** The AP image file name on the TFTP server.

**File Path** The 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 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.

# 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

## *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.

**Format** `show wireless ap [<macaddr>] failure status`

**Mode** Privileged EXEC

**macaddr** The failure AP MAC address.

**MAC Address** The Ethernet address of the AP.

**IP Address** The network IP address of the AP.

**Last Failure Type** Indicates the last type of failure that occurred.

**Validation Failure Count** The count of association failures for this AP.

**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.

# 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

## *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

**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.

**SSID** Service Set ID of the network, this is broadcast in detected beacon frame.

**Physical Mode** Indicates the 802.11 mode being used on the AP.

**Channel** Transmit channel of the AP.

**Transmit Rate** Indicates the rate at which the AP is currently transmitting data.

**Beacon Period** Beacon interval for the neighbor AP network.

**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:

WS Managed - The neighbor AP is managed by this switch, the neighbor AP status can be referenced using its base MAC address.

Peer WS Managed - The neighbor AP is managed by another switch within the peer group.

Standalone - The AP is managed in standalone mode and configured as a valid AP entry (local or RADIUS).

Acknowledged Rogue - The AP is configured as a valid AP entry (local or RADIUS), it has been acknowledged and is not reported as Rogue.

Ad Hoc Rogue - The AP neighbor was detected participating in an ad hoc network.

**Discovered Age** Time in seconds since this AP was first detected in an RF scan.

**Age** Time in seconds since this AP was last detected in an RF scan.

# 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

**macaddr** Client MAC address

## *show wireless client status*

This commands displays summary or detailed data for clients associated to a managed AP.

**Format** `show wireless client [<macaddr>] status`

**Mode** Privileged EXEC

**macaddr** Client MAC address

**MAC Address** The Ethernet address of the client station.

**Tunnel IP Address** This field is blank for all non-tunneled clients. For a tunneled client, this is the assigned tunnel IP address.

**SSID** Indicates the network on which the client is connected.

**VAP MAC Address** Indicates the Ethernet MAC address for the managed AP VAP where this client is associated.

**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.

**Inactive Period** For current association, period of time that the AP has not seen any traffic for the client.

**Age** Indicates the time in seconds since the switch has received new association data for this client.

## *show wireless client statistics*

This command displays association or session statistics for clients currently associated with a switch 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

**macaddr** Switch 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.

**Duplicate Packets Received** Total duplicate packets received from the client station.

**Fragmented Packets Received** Total fragmented packets received from the client station.

**Fragmented Packets 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 client station failed after one or more retries.

## *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

**macaddr** Client MAC address

**MAC Address** The Ethernet address of the client station.

**AP MAC Address** The base Ethernet address of the switch 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 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 with this AP.

### *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

**macaddr** Switch 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.

### *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

**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.

## 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

### *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

**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.

## 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

**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.

# 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*

This command globally enables or disables the captive portal feature on the switch.

**Default** Disable

**Format** `enable`

**Mode** Captive Portal Config Mode

### *no enable*

The `no` version of this command disables the captive portal functionality.

**Default** Disable

**Format** `no enable`

**Mode** Captive Portal Config Mode

## *http port*

This command configures an additional HTTP port. Valid port numbers are in the range of 0-65535.

**Default** 0

**Format** `http port <port-num>`

**Mode** Captive Portal Config Mode

### *no http port*

This command removes the specified additional HTTP port.

**Format** no `http port <port-num>`

**Mode** Captive Portal Config Mode

## statistics interval

Use this command to configure the interval at which statistics are reported to the cluster controller. The **<interval>** variable is the reporting interval, which is a number in the range of 15-3600 seconds.

**Default** 120

**Format** **statistics interval** *<interval>*

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #statistics interval 200<cr>
```

### no statistics interval

Use this command to set the statistics interval to the default value.

**Format** **no statistics interval <interval>**

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #no statistics interval<cr>
```

## 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, which is a number in the range of 60-600 seconds.

**Default** 300

**Format** **authentication timeout** *<timeout>*

**Mode** Captive Portal Config Mode

### no authentication timeout

This command configures sets the authentication timeout to the default value.

**Format** **no authentication timeout**

**Mode** Captive Portal Config Mode

## show captive-portal

This command reports status of the captive portal feature.

**Format** **show captive-portal**

**Mode** Privileged EXEC

**Administrative Mode** Shows whether the CP is enabled.

**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

**Authenticated Users** Shows the number of users currently authenticated to all captive portal instances on this switch.

**System Supported Users** Shows the number of authenticated users that the system can support.

**Configured Captive Portals** Shows the number of captive portals configured on the switch.

**Supported Captive Portals** Shows the number of supported captive portals in the system.

**Active Captive Portals.** Shows the number of captive portal instances that are operationally enabled.

## 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 *<cp-id>* variable is a number in the range of 1-10.

**Format** `configuration` *<cp-id>*

**Mode** Captive Portal Config Mode

#### *no configuration*

This command deletes a captive portal configuration. The command fails if interfaces are associated to this configuration. The default captive portal configuration can not be deleted.

**Format** `no configuration` *<cp-id>*

**Mode** Captive Portal Config Mode

### *enable (Captive Portal)*

This command enables a captive portal configuration.

**Default** Enable

**Format** `[no] enable`

**Mode** Captive Portal Instance Mode

### *no enable*

This command disables a captive portal configuration.

**Default** Enable

**Format** `no enable`

**Mode** Captive Portal Instance Mode

## *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 Mode

## *protocol*

This command configures the protocol mode for a captive portal configuration. The CP can use HTTP or HTTPS.

**Default** https

**Format** `protocol {http | https}`

**Mode** Captive Portal Instance Mode

## *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 Mode

## *group*

This command configures the group name for a captive portal configuration. If a group name is configured the user entry (Local or RADIUS) must be configured with the same group name to authenticate to this captive portal instance. The name can contain up to 32 alphanumeric characters.

**Format** `group <group-name>`

**Mode** Captive Portal Instance Mode

## radius accounting

This command enables radius accounting for a captive portal configuration.

**Default** Disable

**Format** `radius accounting`

**Mode** Captive Portal Instance Mode

### no radius accounting

This command disables radius accounting for a captive portal configuration.

**Default** Disable

**Format** `no radius accounting`

**Mode** Captive Portal Instance Mode

## redirect-url mode

This command enables or disables the redirect mode for a captive portal configuration.

**Default** Disable

**Format** `redirect-url mode`

**Mode** Captive Portal Instance Mode

### no redirect-url mode

This command disables the redirect mode for a captive portal configuration.

**Format** `no redirect-url mode`

**Mode** Captive Portal Instance Mode

## 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 is the redirect mode is enabled.

**Format** `redirect-url <url>`

**Mode** Captive Portal Instance Mode

## rate-limit up

Use this command to configure the maximum rate at which a client can send data into the network.

**Default** 0

**Format** **rate-limit up** *<rate>*

**Mode** Captive Portal Instance Mode

**Rate** Rate in bps. 0 indicates the limit is not enforced.

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #rate-limit up 100<cr>
```

### *no rate-limit up*

Use this command to set the rate-limit up to the default value.

**Format** **no rate-limit up**

**Mode** Captive Portal Instance Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #no rate-limit up<cr>
```

## *rate-limit down*

Use this command to configure the maximum rate at which a client can receive data from the network.

**Default** 0

**Format** **rate-limit down** *<rate>*

**Mode** Captive Portal Instance Mode

**Rate** Rate in bps. 0 indicates the limit is not enforced.

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #rate-limit down 100<cr>
```

### *no rate-limit down*

Use this command to set the rate-limit down to the default value.

**Format** **no rate-limit down**

**Mode** Captive Portal Instance Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #no rate-limit up<cr>
```

## *rate-limit input-octets*

Use this command to configure 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** **rate-limit input-octets** *<bytes>*

**Mode** Captive Portal Instance Mode

**Bytes** Input octets in bytes. 0 indicates the limit is not enforced.

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #rate-limit input-octets 100<cr>
```

### *no rate-limit input-octets*

Use this command to set the rate-limit input-octets to the default value.

**Format** **no rate-limit input-octets**

**Mode** Captive Portal Instance Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #no rate-limit input-octets<cr>
```

## *rate-limit output-octets*

Use this command to configure 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** **rate-limit output-octets** *<bytes>*

**Mode** Captive Portal Instance Mode

**Bytes** Output octets in bytes. 0 indicates the limit is not enforced.

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #rate-limit output-octets 100<cr>
```

### *no rate-limit output-octets*

Use this command to set the rate-limit output-octets to the default value.

**Format** **no rate-limit output-octets**

**Mode** Captive Portal Instance Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #no rate-limit output-octets<cr>
```

## *rate-limit total-octets*

Use this command to configure 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** **rate-limit total-octets** *<bytes>*

**Mode** Captive Portal Instance Mode

**Bytes** Total octets in bytes. 0 indicates the limit is not enforced.

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #rate-limit total-octets 100<cr>
```

### *no rate-limit total-octets*

Use this command to set the rate-limit total-octets to the default value.

**Format** **no rate-limit total-octets**

**Mode** Captive Portal Instance Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #no rate-limit total-octets<cr>
```

## *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 Mode

### *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 Mode

## *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 Mode

### *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 Mode

## intrusion-threshold

This command configures the minimum trap interval for reporting authentication failures for a captive portal configuration. The *<time>* variable is a number that represents the intrusion threshold in seconds. Use 0 to indicate that no traps are sent.

**Default** 0

**Format** `intrusion-threshold` *<time>*

**Mode** Captive Portal Instance Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #intrusion-threshold 600<cr>
```

### no intrusion-threshold

Use this command to set the trap interval for reporting authentication failures for a captive portal configuration to the default value.

**Format** `intrusion-threshold` *<time>*

**Mode** Captive Portal Instance Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #no intrusion-threshold<cr>
```

## locale

This command is not intended to be a user command. The administrator must use the WEB UI to create and customize captive portal web content. This command is primarily used by the FASTPATH 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> <content>*

**Mode** Captive Portal Instance Mode

## 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 Config Mode

### no interface

This command removes the association between an interface and a captive portal configuration.

**Format** `no interface` *<slot/port>*

**Mode** Captive Portal Instance Config Mode

### *block*

This command blocks all traffic for a captive portal configuration.

**Format** `block`

**Mode** Captive Portal Instance Config Mode

*no block*

This command unblocks all traffic for a captive portal configuration.

**Format** `no block`

**Mode** Captive Portal Instance Config Mode

## 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

**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.

### *show captive-portal configuration interface*

This command displays information of 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` *[slot/port]*

**Mode** Privileged EXEC

**CP ID** Shows the captive portal ID

**CP Name** Shows the captive portal name

**Intf** Valid slot and port number separated by forward slashes.

**Intf Description** Describes the interface.

**Oper Status** Shows whether the captive portal is enabled or disabled

**Blocked 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.

**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

**CP ID** Shows the captive portal ID

**CP Name** Shows the captive portal name

**Mode** Shows whether the CP is enabled or disabled

**Protocol** Shows the current connection protocol, which is either HTTP or HTTPS

**Verification** 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:

**Group Name** Identifies the group to which the user belongs.

**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.

**RADIUS Accounting** Indicates whether RADIUS Accounting is enabled or disabled

**Redirect URL Mode** Indicates whether the Redirect URL Mode is enabled or disabled

**Redirect URL** Specifies the URL to which the newly authenticated client is redirected if the URL Redirect Mode is enabled.

## show captive-portal configuration locales

This command displays locales associated with a specific captive portal configuration.

**Format** `show captive-portal configuration locales`

**Mode** Privileged EXEC

**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.

**Language Code** Shows the language code.

**Local Link** Shows the local description.

# 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 a client, to view additional information about that client.

**Format** `show captive-portal client` *[macaddr]* `status`

**Mode** Privileged EXEC

**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** Shows the current connection protocol, which is either HTTP or HTTPS

**Verification** 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 forward slashes.

**Interface Description** Describes the interface.

**User Name** Displays the user name (or Guest ID) of the connected client

## *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

**Client MAC Address** Identifies the MAC address of the wireless client (if applicable)

**Bytes Transmitted** Total bytes the client has transmitted

**Bytes Received** Total bytes the client has received

**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

**Intf** Valid slot and port number separated by forward slashes.

**Intf 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)

**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.

**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.

**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

**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:

**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.

**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 forward slashes.

**Interface Description** Describes the interface.

**User Name** Displays the user name (or Guest ID) of the connected client

## show captive-portal client failure status

This command displays a summary of authorization failures or detailed information for a specific failure.

**Format** `show captive-portal client [macaddr] failure status`

**Mode** Privileged EXEC

**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.

**Attempts** Shows the number of times the client has unsuccessfully tried to log on to the captive portal.

**Last Attempt** Shows the time when the client last tried to log on.

If you use the optional `[macaddr]` information, the following additional information appears:

**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 forward slashes.

**Interface Description** Describes the interface.

**User Name** Displays the user name (or Guest ID) of the connected client

**Creation Time** Displays the time when the user was configured in the local database.

## clear captive-portal client failure

This command deletes all the entries from the client authorization failure list.

**Format** `clear captive-portal client failure`

**Mode** Privileged EXEC

## captive-portal client deauthenticate

This command deauthenticates a specific captive portal client. The `<macaddr>` variable is the MAC address of the client to deauthenticate.

**Format** `captive-portal client deauthenticate <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

**Intf** Valid slot and port number separated by forward slashes.

**Intf Description** Describes the interface.

**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.

**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

**Intf** Valid slot and port number separated by forward slashes.

**Intf Description** Describes the interface.

**Type** Shows the type of interface.

# Captive Portal Local User Commands

Use this command to view and configure captive portal users in the local database.

## *user*

This command is used to create a local user. The ***<user-id>*** variable is the user ID, which can be up to 128 alphanumeric characters. 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.

**Format** **user *<user-id>* password *<password>***

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #user 1 password test1234<cr>
```

### *no user*

This command deletes a user from local user database. If the user has an existing session, it is disconnected.

**Format** **no user** *<user-id>*

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #no user 1<cr>
```

## *user password encrypted*

This command modifies the password for the associated captive portal user. The command accepts the password in an encrypted format.

The *<encrypt-pwd>*variable is the password in encrypted format, which can be up to 128 hexadecimal characters

**Format** **user <user-name> password encrypted <encrypted-pwd>**

**Mode** Captive Portal Config Mode

## *user group*

This command modifies the group name for the associated captive portal user. The ***<user-id>*** variable is the user ID, which can be up to 128 alphanumeric characters. The ***<group-name>*** variable is the group name, which can be up to 32 alphanumeric characters.

**Format** **user <user-id> group <group-name>**

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #user 1 group group123<cr>
```

## user session-timeout

This command sets the session timeout value for the associated captive portal user. The *<user-name>* variable is a user configured in the local database. 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-name>* **session-timeout** *<timeout>*

**Mode** Captive Portal Config Mode

### no user session-timeout

This command sets the session timeout value for the associated captive portal user to the default value. The *<user-name>* variable is a user configured in the local database.

**Format** **no user** *<user-name>* **session-timeout**

**Mode** Captive Portal Config Mode

## user idle-timeout

This command sets the session idle timeout value for the associated captive portal user. The *<user-name>* variable is a user configured in the local database. 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-name>* **idle-timeout** *<timeout>*

**Mode** Captive Portal Config Mode

### no user idle-timeout

This command sets the session idle timeout value for the associated captive portal user to the default value. The *<user-name>* variable is a user configured in the local database.

**Format** **user** *<user-name>* **idle-timeout** *<timeout>*

**Mode** Captive Portal Config Mode

## user rate-limit up

Use this command to configure the bandwidth at which the client can send data into the network. 0 denotes using the default value configured for the captive portal. The ***<user-id>*** variable is the user ID, which can be from 1 to 128 alphanumeric characters. The ***<bps>*** variable is the client transmit rate in bits per second (bps). 0 denotes unlimited bandwidth.

**Default** 0

**Format** **user** *<user-id>* **rate-limit up** *<bps>*

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #user 1 rate-limit up 128000<cr>
```

### *no user rate-limit up*

This command sets the user rate-limit up to the default value.

**Format** **no user** *<user-id>* **rate-limit up**

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #no user 1 rate-limit up<cr>
```

## *user rate-limit down*

Use this command to configure the bandwidth at which the client can receive data from the network. 0 denotes using the default value configured for the captive portal. The ***<user-id>*** variable is the user ID, which can be from 1 to 128 alphanumeric characters. The ***<bps>*** variable is the client receive rate in bits per second (bps). 0 denotes unlimited bandwidth.

**Default** 0

**Format** **user** *<user-id>* **rate-limit down** *<bps>*

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #user 1 rate-limit down 128000<cr>
```

### *no user rate-limit down*

This command sets the user rate-limit down to the default value.

**Format** **no user** *<user-id>* **rate-limit down**

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #no user 1 rate-limit down<cr>
```

## *user rate-limit input-octets*

Use this command to limit the number of octets the user is allowed to transmit. After this limit has been reached, the user will be disconnected. 0 octets denote unlimited transmission. The

***<user-id>*** variable is the user ID, which can be from 1 to 128 alphanumeric characters. The ***<octets>*** variable is the number of bytes.

**Default** 0

**Format** **user** *<user-id>* **rate-limit input-octets** *<octets>*

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #user 1 rate-limit input-octets 100<cr>
```

### *no user rate-limit input-octets*

This command sets the user rate-limit input-octets to the default value.

**Format** **no user** *<user-id>* **rate-limit input-octets**

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #no user 1 rate-limit input-octets<cr>
```

## *user rate-limit output-octets*

Use this command to limit the number of octets the user is allowed to receive. After this limit has been reached, the user will be disconnected. 0 octets denote unlimited transmission. The ***<user-id>*** variable is the user ID, which can be from 1 to 128 alphanumeric characters. The ***<octets>*** variable is the number of bytes.

**Default** 0

**Format** **user** *<user-id>* **rate-limit output-octets** *<octets>*

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #user 1 rate-limit output-octets 100<cr>
```

### *no user rate-limit output-octets*

This command sets the user rate-limit output-octets to the default value.

**Format** **no user** *<user-id>* **rate-limit output-octets**

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #no user 1 rate-limit output-octets<cr>
```

## user rate-limit total-octets

Use this command to limit the number of bytes 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. The ***<user-id>*** variable is the user ID, which can be from 1 to 128 alphanumeric characters. The ***<octets>*** variable is the number of bytes.

**Default** 0

**Format** **user** *<user-id>* **rate-limit total-octets** *<octets>*

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #user 1 rate-limit total-octets 100<cr>
```

### no user rate-limit total-octets

This command sets the user rate-limit total-octets to the default value.

**Format** **no user** *<user-id>* **rate-limit total-octets**

**Mode** Captive Portal Config Mode

***Example:*** The following shows an example of the command.

```
(Switch)(Config-CP) #no user 1 rate-limit total-octets<cr>
```

## show captive-portal user

This command displays all configured users or a specific user in the captive portal local user database. Enter the optional username to view information about the specified user. The ***[user-name]*** variable is a valid user configured in the local database.

**Format** **show captive-portal user** ***[user-name]***

**Mode** Privileged EXEC

**User** Displays the user name

**Group** Displays the group to which the user belongs

**Session Timeout** Displays the number of seconds

**Idle Timeout** Displays the number of seconds

When you specify a user with the optional *[user-name]* variable, the following information displays:

**User** Displays the user name

**Password Configured.** Indicates whether a password is configured for the user

**Group Name** Displays the group to which the user belongs

**Session Timeout** Displays the number of seconds

**Idle Timeout** Displays the number of seconds

### *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 Mode

*no user group*

Use this command to delete a user group.

**Format** `no user group <group-name>`

**Mode** Captive Portal Config Mode

### *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 Mode

### *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 Mode

## Captive Portal Activity Log Commands

Use the commands in this section to view or clear the activity log for the captive portals.

## show captive-portal activity-log

This command displays the information in the captive portal activity log.

**Format** `show captive-portal activity-log`

**Mode** Privileged EXEC

## clear captive-portal activity-log

This command deletes all entries from the captive portal activity log.

**Format** `clear captive-portal activity-log`

**Mode** Privileged EXEC

# 5

# Quality of Service (QoS) Commands

This chapter describes the Quality of Service (QoS) commands available in the D-Link Unified Wired/Wireless Access System CLI.

The QoS Commands chapter contains the following sections:



The commands in this chapter are in one of two functional groups:

- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Show commands are used to display device settings, statistics and other information.

## Class of Service (CoS) 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 "Provisioning (IEEE 802.1p) Commands" on page 64.

**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), IP DSCP, or IP Precedence 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 | ip-precedence | untrusted}`

**Mode** 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 platform specific. 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-n>`

**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-1> [<queue-id-2> … <queue-id-n>]`

**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-1> [<queue-id-2> … <queue-id-n>]`

**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 and is only valid on platforms that support independent per-port class of service mappings. 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 "Provisioning (IEEE 802.1p) Commands" on page 64.

**Format** `show classofservice dot1p-mapping` *[<slot/port>]*

**Mode** Privileged EXEC

The following information is repeated for each user priority.

**User Priority** The 802.1p user priority value.

**Traffic Class** The traffic class internal queue identifier to which the user priority value is mapped.

## *show classofservice ip-precedence-mapping*

This command displays the current IP Precedence mapping to internal traffic classes for a specific 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 IP Precedence mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

**Format** `show classofservice ip-precedence-mapping` *[<slot/port>]*

**Mode** Privileged EXEC

The following information is repeated for each user priority.

**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.

**IP DSCP** The IP DSCP value.

**Traffic Class** The traffic class internal queue identifier to which the IP DSCP value is mapped.

## show classofservice trust

This command displays the current trust mode setting for a specific interface. The *<slot/port>* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. 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

**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'.

## 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

**Queue Id** An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.

**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.

**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.

# Differentiated Services (DiffServ) 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
   - Creating and deleting classes.
   - Defining match criteria for a class.
2. Policy
   - Creating and deleting policies
   - Associating classes with a policy
   - Defining policy statements for a policy/class combination
3. Service
   - 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.

**NOTE:** Traffic to be processed by the DiffServ feature requires an IP 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.

**NOTE:** The CLI mode is changed to Class-Map Config 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 (The `<class-map-name>` 'default' is reserved and must not be used here).

**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. There is no default value.

**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 attempts 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 a platform-specific maximum. 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, and *<ippmask>* specifies a subnet 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

## *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

## 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

### 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 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

# 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 *n*-1, where *n* is the number of egress queues supported by the device.

**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), Police

## 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

**Policy Type** In

**Incompatibilities** Drop, Mark CoS, Mark IP DSCP, 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:

**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.

**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:

**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.

## 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

**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:

**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):

**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.

**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:

**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.

## *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

**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 forward slashes.

**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).

## 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

**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):

**Interface** Valid slot and port number separated by forward slashes.

**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.

## 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

**Interface** Valid slot and port number separated by forward slashes.

**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:

**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.

### *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):

**Interface** Valid slot and port number separated by forward slashes.

**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 (ACL) Commands

This section describes the commands you use to configure MAC 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 create is 100, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is hardware dependent.
- 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}

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:** For assign-queue, 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, 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 |
| 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-(n-1), where n is the number of user configurable queues available for the hardware platform. The *assign-queue* parameter is valid only for a **permit** rule.

The *assign-queue* and *redirect* parameters are only valid for a **permit** rule.

**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>]]*

**Mode** Mac-Access-List Config

## *mac access-group*

This command attaches a specific MAC Access Control List (ACL) identified by *<name>* to an interface 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 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration.

**Format** **mac access-group** *<name>* **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-list** *<name>* **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

**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.

# IP Access Control List (ACL) Commands

This section describes the commands you use to configure IP 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:

- D-Link Unified Wired/Wireless Access System software does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is 100, regardless of type.
- The maximum number of rules per IP ACL is hardware dependent.
- On current platforms, 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>]*

**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>]*

**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.<br><br>Note: For assign-queue, 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. |

### *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-group

This command attaches a specified IP ACL to one interface or to all interfaces.

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> 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> in`

**Mode** Interface 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.

**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.

## *show access-lists*

This command displays IP ACLs and MAC access control lists information for a designated interface and direction.

**Format** `show access-lists interface <slot/port> in`

**Mode** Privileged EXEC

**ACL Type** Type of access list (IP or MAC).

**ACL ID** Access List name for a MAC 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).

# 6

# Utility Commands

This chapter describes the utility commands available in the D-Link Unified Wired/Wireless Access System CLI.

The Utility Commands chapter includes the following sections:



The commands in this chapter 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.

## Power Over Ethernet Commands

This section describes the Power over Ethernet (PoE) commands available in the D-Link Unified Wired/Wireless Access System CLI.

**NOTE:** When a port starts or stops delivering power to a connected device, there will be a trap indicating the change.

### *poe limit*

Use this command in Global Config mode to set the power limit (in watts) for all ports. Use the command in Interface Config mode to set the power limit for a specific port. The port will not supply more power than the value specified as the limit.

**Default** 16.8

**Format** `poe limit <1-18>`

**Mode** Global Config
Interface Config

### *no poe limit*

This command resets the power limit for all ports (Global Config) or a specific port (Interface Config) to the default.

**Format** `no poe limit`

**Mode** Global Config
Interface Config

## *poe priority*

Use this command to set the priority level for all ports (Global Config mode) or for a specific port (Interface Config mode) for the delivery of power to an attached device. The switch may not be able to supply power to all connected devices, so the port priority is used to determine which ports will supply power if adequate power capacity is not available for all enabled ports. For ports that have the same priority level, the lower numbered port will have higher priority.

**Default** low

**Format** `poe priority {low | high | critical}`

**Mode** Global Config
Interface Config

### *no poe priority*

This command resets the priority level to the default.

**Format** `no poe priority`

**Mode** Global Config
Interface Config

## *poe usagethreshold*

This command sets the power threshold level at which a trap will be generated. If the total power consumed is greater than or equal to the specified percentage of the total power available, a trap will be sent. Valid values are 0-100 percent.

**Default** 80

**Format** `poe usagethreshold <0-100>`

**Mode** Global Config

### *no poe usagethreshold*

This command resets the usage threshold for all ports to the default

**Format** `no poe usagethreshold`

**Mode** Global Config

## show poe

This command displays the total power available, the total power consumed in the system, and the globally set usage threshold.

**Format** `show poe`

**Mode** Privileged EXEC

**Total Power Available** Amount of power available, in watts.

**Total Power Consumed** Power consumed, in watts.

**Usage Threshold** Allowed power level threshold before a trap is generated.

## show poe port

Use this command with the *all* keyword to display PoE information for all ports that support the PoE function. Use the command with the *<slot/port>* variable to display PoE information for a specific port. If a port does not have link or is not enabled for PoE, the fields display a value of "N/A."

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

**Mode** Privileged EXEC

**Slot/Port** The slot and port number associated with the rest of the data in the row.

**Admin Mode** The admin mode of the port.

**Class** The class of the powered device according to IEEE802.3af definition, as shown in the following table:

| Class | Usage | Max Power |
|---|---|---|
| 0 | Default | 0.44-12.95 |
| 1 | Optional | 0.44-3.84 |
| 2 | Optional | 3.84-6.49 |
| 3 | Optional | 6.49-12.95 |
| 4 | Not Allowed | Reserved |

**Priority** The priority defined by the `poe priority` command, which can be low, high, or critical.

**Output Power** The power supplied to the powered device (in watts).

**Output Current** The current supplied to the powered device (in ma).

**Output Voltage** The voltage applied to the powered device (in volts).

**Limit** The preset limit defined by the `config poe port limit` command. This value is stated in watts.

**Status** The state of power supplied to the associated port. Possible values are Disabled, Searching, Delivering Power, Fault, Test, Other Fault

# Dual Image Commands

D-Link Unified Wired/Wireless Access System 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. The command also displays any text description associated with an image. This command displays the switch activation status.

**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 - network or service ports. ARP entries associated with routing interfaces are not listed.

**Format** `show arp switch`

**Mode** Privileged EXEC

**IP Address** IP address of the management interface or another device on the management network.

**MAC Address** Hardware MAC address of that device.

**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

**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.

**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 "show version" command.

**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

**Switch Description** Text used to identify the product name of this switch.

**Machine Type** The machine model as defined by the Vital Product Data.

**Machine Model** The machine model as defined by the Vital Product Data.

**Serial Number** The unique box serial number for this switch.

**FRU Number** The field replaceable unit number.

**Part Number** Manufacturing part number.

**Maintenance Level** Hardware changes that are significant to software.

**Manufacturer** Manufacturer descriptor field.

**Burned in MAC Address** Universally assigned network address.

**Software Version** The release.version.revision number of the code currently running on the switch.

**Operating System** The operating system currently running on the switch.

**Network Processing Device** The type of the processor microcode.

**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>*, is as follows:

**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" is as follows:

**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.

**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:

**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.

**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.

**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.

**Received Packets Not Forwarded**

**Total** - A count of valid frames received which were discarded (in other words, filtered) by the forwarding process.

**Local Traffic Frames** - The total number of frames dropped in the forwarding process because the destination address was located off of this port.

**802.3x Pause Frames Received** - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

**Unacceptable Frame Type** - The number of frames discarded from this port due to being an unacceptable frame type.

**Multicast Tree Viable Discards** - The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.

**Reserved Address Discards** - The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.

**Broadcast Storm Recovery** - The number of frames discarded that are destined for FF:FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled.

**CFI Discards** - The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.

**Upstream Threshold** - The number of frames discarded due to lack of cell descriptors available for that packet's priority level.

**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.

**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 Collisions** - A count of frames for which transmission on a particular interface fails due to excessive collisions.

**Late Collision Frames** - 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:

**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.

**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.

**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:

**VLAN ID** The VLAN on which the MAC address was learned.

The following information displays if you enter the *count* parameter:

**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 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.

**Format** **show running-config** *[all | <scriptname>]*

**Mode** Privileged EXEC

## show sysinfo

This command displays switch information.

**Format** **show sysinfo**

**Mode** Privileged EXEC

**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 310.

**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 310.

**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 310.

**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 logging`**
- **`show event log`**
- **`show logging buffered`**
- **`show trap log`**
- **`show running config`**

**Format** **`show tech-support`**

**Mode** Privileged EXEC

# 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 D-Link Unified Wired/Wireless Access System 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>* is the IP address of the logging host. 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> [<port>][<severitylevel>]*

**Mode** Global Config

## logging host remove

This command disables logging to host. See "show logging hosts" on page 271 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

**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.

**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

**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.

**Format** `show logging hosts`

**Mode** Privileged EXEC

**Host Index** (Used for deleting hosts)

**IP Address** IP address 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

**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. The *<ipaddr>* value should be a valid IP address. The *[<port>]* value should be a valid decimal integer in the range of 0 (zero) to 65535. The optional port parameter is the UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system. The default value is 33434.

**Format** **traceroute** *<ipaddr> [<port>]*

**Mode** Privileged EXEC

### *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 eight alphanumeric characters. The password is case sensitive.

**Format** `enable passwd`

**Mode** User 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

This command checks if another computer is on the network and listens for connections. To use this command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. You can ping the switch from any IP workstation the switch is connected to through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station.

**Format** `ping <ipaddr>`

**Modes** Privileged EXEC
User EXEC

## 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. **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>/<filepath>/<filename>}*

For TFTP, the *<ipaddr>* parameter is the IP address of the server, *<filepath>* is the path to the file, and *<filename>* is the name of the file you want to upload or download.

**Table 11. Copy Parameters**

| Source | Destination | Description |
|---|---|---|
| *nvram:clibanner* | *<url>* | Copies the CLI banner to a server. |
| *nvram:errorlog* | *<url>* | Copies the error log 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* | *<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: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:sshkey-dsa* | Downloads an SSH key file. For more information, see "Secure Shell (SSH) Command" on page 302. |
| *<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**

| Source | Destination | Description |
|---|---|---|
| *<url>* | *nvram:sslpem-root* | Downloads an HTTP secure-server certificate. For more information, see "Hypertext Transfer Protocol (HTTP) Commands" on page 304. |
| *<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**. |

# Keying for Advanced Features

This section describes the commands you use to enter the licence key to access advanced features. You cannot access the advanced features without a valid license key.

## *license advanced*

This command enables a particular feature. This command also enables the corresponding show commands for a feature.

**NOTE:** If the feature is enabled, the feature is visible in the output of the **show running-config** command. The *<key>* parameter specifies the hexadecimal key for the feature.

**Default** none

**Format** **license advanced** *<key>*

**Mode** Privileged EXEC

### *no license advanced*

This command disables a particular feature. This command also disables the corresponding show commands. The *<key>* parameter specifies the hexadecimal key for the feature.

**Format** **no license advanced** *<key>*

**Mode** Privileged EXEC

## *show key-features*

This command displays the enabled or disabled status for all keyable features.

**Format** `show key-features`

**Modes** Privileged EXEC
User EXEC

**Function** This is the name of the keyable component or feature.

**Status** Enabled or disabled.

# Simple Network Time Protocol (SNTP) Commands

This section describes the commands you use to automatically configure the system time and date by using SNTP.

## *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> [<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>*

**Mode** Global Config

## *show sntp*

This command is used to display SNTP settings and status.

**Format** `show sntp`

**Mode** Privileged EXEC

**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.

**Multicast Count** Current number of unsolicited multicast 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

**Client Supported Modes** Supported SNTP Modes (Broadcast, Unicast, or Multicast).

**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

**Server IP Address** IP address 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:

**IP Address** IP address 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.

# 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 IP 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 1439. *Minutes* is an integer from 0 to 86399.

**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.type Specifies the NetBIOS node type. 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

**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

**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

**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:

**Network** The network number and the mask for the DHCP address pool.

The following additional fields are displayed for Manual pool type:

**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

**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:

**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:

**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

**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.

# DHCP Filtering

You can configure the DHCP Filtering feature as a security measure against unauthorized DHCP servers. DHCP filtering works by allowing you to configure each port as either a trusted port or an untrusted port. To optimize the DHCP filtering feature, configure the port that is connected to an authorized DHCP server on your network as a trusted port. Any DHCP

responses received on a trusted port are forwarded. Make sure that all other ports are untrusted so that any DHCP (or BootP) responses received are discarded.

You can configure DHCP filtering on physical ports and LAGs. DHCP filtering is not operable on VLAN interfaces.

## ip dhcp filtering

This command enables DHCP filtering globally.

**Default** disabled

**Format** `ip dhcp filtering`

**Mode** Global Config

### no ip dhcp filtering

This command disables DHCP filtering.

**Format** `no ip dhcp filtering`

**Mode** Global Config

## ip dhcp filtering trust

This command configures an interface as trusted.

**Default** untrusted

**Format** `ip dhcp filtering trust`

**Mode** Interface Config

### no ip dhcp filtering trust

This command returns an interface to the default value for DHCP filtering.

**Format** `no ip dhcp filtering trust`

**Mode** Interface Config

## show ip dhcp filtering

This command displays the DHCP filtering configuration.

**Format** `show ip dhcp filtering`

**Mode** Privileged EXEC

**Interface** The interface by slot/port.

**Trusted** Indicates whether the interface is trusted or untrusted.

# 7

# Management Commands

This chapter describes the management commands available in the D-Link Unified Wired/ Wireless Access System CLI.

The Management Commands chapter contains the following sections:



The commands in this chapter are divided into 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.
- Copy commands transfer or save configuration and informational files to and from the switch.

## 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 53

### *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

## serviceport ip

This command sets the IP address, the netmask and the gateway of the network management port.

**Format** `serviceport ip <ipaddr> <netmask> [gateway]`

**Mode** Privileged EXEC

## serviceport protocol

This command specifies the network management port configuration protocol. If you modify this value, the 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.

**Format** `serviceport protocol {none | bootp | dhcp}`

**Mode** Privileged 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 EXE

## 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. When access is enabled, the Java applet can be viewed from the Web interface. When access is disabled, the user cannot view the Java applet.

**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.

**Format** `show network`

**Modes** Privileged EXEC
User EXEC

**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.

**Network Configuration Protocol Current** The network protocol being used. The options are bootp | dhcp | none.

**Java Mode** Specifies if the switch should allow access to the Java applet in the header frame. Enabled means the applet can be viewed. The factory default is enabled.

**Web Mode** Specifies if the switch should allow access to the Web Interface. The factory default is enabled.

## *show serviceport*

This command displays service port configuration information.

**Format** `show serviceport`

**Mode** Privileged EXEC

**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

**ServPort Configuration Protocol Current** The network protocol used on the last, or current power-up cycle, if any.

**Burned in MAC Address** The burned in MAC address used for in-band connectivity.

# 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

**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. 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 <host> <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

**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

**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 (SSH) Command

This section describes the commands you use to configure 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.

**Default** disabled

**Format** `ip ssh`

**Mode** Privileged EXEC

#### *no ip ssh*

Use this command to disable SSH access to the system.

**Format** `no 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

**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.

**Connections** This field specifies the current SSH connections.

# Hypertext Transfer Protocol (HTTP) Commands

This section describes the commands you use to configure 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 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

**HTTP Mode (Unsecure)** The unsecure HTTP server administrative mode.

**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

# 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 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

**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.

**Session Time** Total time this session has been connected.

**Session Type** Shows the type of session, which can be telnet, serial, or SSH.

# User Account Commands

This section describes the commands you use to add, manage, and delete system users. D-Link Unified Wired/Wireless Access System 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 passwd*

Use this command to change a password. Passwords are a maximum of eight 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 326.

**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

## *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

## 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.

**Default** 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

**User Name** The name the user enters to login using the serial port, Telnet or Web.

**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.

# 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

This command restricts access to switch information. The access mode is read-only (also called public).

**Format** `snmp-server community ro <name>`

**Mode** Global Config

## 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 65.

**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 Flag.

**Default** enabled

**Format** `snmp-server enable traps`

**Mode** Global Config

### no snmp-server enable traps

This command disables the Authentication Flag.

**Format** `no snmp-server enable traps`

**Mode** Global Config

## snmp-server enable traps bcaststorm

This command enables the broadcast storm trap. When enabled, broadcast storm traps are sent only if the broadcast storm recovery mode setting associated with the port is enabled.

**NOTE:** This command may not be available on all platforms.

**Default** enabled

**Format** `snmp-server enable traps bcaststorm`

**Mode** Global Config

### *no snmp-server enable traps bcaststorm*

This command disables the broadcast storm trap. When enabled, broadcast storm traps are sent only if the broadcast storm recovery mode setting associated with the port is enabled.

**NOTE:** This command may not be available on all platforms.

**Format** `no snmp-server enable traps bcaststorm`

**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 315.

**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.

**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 page39."

**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 313.

**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 313.

**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 313.

**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

**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

**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 IP address to receive SNMP traps from this device.

**Status** The receiver's status (enabled or disabled).

## *show trapflags*

This command displays trap conditions. Configure which traps the switch should generate 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

**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.

**Broadcast Storm Flag** Can be enabled or disabled. The factory default is enabled. Indicates whether broadcast storm traps are sent.

**ACL Traps** May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.

**BGP4 Traps** Can be enabled or disabled. The factory default is disabled. Indicates whether BGP4 traps are sent. (This field appears only on systems with the BGPv4 software package installed.)

**DVMRP Traps** Can be enabled or disabled. The factory default is disabled. Indicates whether DVMRP traps are sent.

**OSPF Traps** Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent.

**PIM Traps** Can be enabled or disabled. The factory default is disabled. Indicates whether PIM traps are sent.

# 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.

## *radius accounting mode*

This command is used to enable the RADIUS accounting function.

**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 host*

This command is used to configure the RADIUS authentication and accounting server. If you use the *<auth>* parameter, the command configures the IP address to use to connect to a RADIUS authentication server. You can configure up to 3 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 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 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 1 - 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> [<port>]*

**Mode** Global Config

### *no radius server host*

This command is used to remove the configured RADIUS authentication server or the RADIUS accounting server. 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>* parameter must match the IP address of the previously configured RADIUS authentication / accounting server.

**Format** **no radius server host** *{auth | acct} <ipaddress>*

**Mode** Global Config

## *radius server attribute 4*

Use this command to enable the Radius Attribute 4 (NAS-IP Address) inclusion in RADIUS requests. Use the optional *[ipaddr]* variable to explicitly include the IP address to be sent as the NAS-IP address to the RADIUS servers. If you do not specify a value for the *[ipaddr]* variable, then the outgoing interface IP address that is used to send the packet to the RADIUS server is added as NAS-IP Address.

**Default** disabled

**Format** **radius server attribute 4** *[ipaddr]*

**Mode** Global Config

### *no radius server attribute 4*

Use this command to disable the Radius Attribute 4 (NAS-IP Address) inclusion in RADIUS requests.

**Format** **radius server attribute 4**

**Mode** Global Config

## *radius server key*

This command is used to configure the shared secret between the RADIUS client and the RADIUS accounting / authentication 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 provided must match a previously configured server. When this command is executed, the secret is prompted.

**NOTE:** The secret must be an alphanumeric value not exceeding 16 characters.

**Format** **radius server key** *{auth | acct} <ipaddr>*

**Mode** Global Config

## *radius server msgauth*

This command enables the message authenticator attribute for a specified server.

**Format** **radius server msgauth** *<ipaddr>*

**Mode** Global Config

### *no radius server msgauth*

This command disables the message authenticator attribute for a specified server.

**Format** `no radius server msgauth <ipaddr>`

**Mode** Global Config

## *radius server primary*

This command is used to configure the primary RADIUS authentication server for this RADIUS client. The primary server handles RADIUS requests. The remaining configured servers are only used if the primary server cannot be reached. You can configure up to three servers on each client. Only one of these servers can be configured as the primary. If a primary server is already configured prior to this command being executed, the server specified by the IP address specified used in this command will become the new primary server. The IP address must match that of a previously configured RADIUS authentication server.

**Format** `radius server primary <ipaddr>`

**Mode** Global Config

## *radius server retransmit*

This command sets the maximum number of times a request packet is re-transmitted when no response is received from the RADIUS server. The retries value is an integer in the range of 1 to 15.

**Default** 4

**Format** `radius server retransmit <retries>`

**Mode** Global Config

### *no radius server retransmit*

This command sets the maximum number of times a request packet is re-transmitted, to the default value.

**Format** `no radius server retransmit`

**Mode** Global Config

## *radius server timeout*

This command sets 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

### *no radius server timeout*

This command sets the timeout value to the default value.

**Format** `no radius server timeout`

**Mode** Global Config

## *authorization network radius*

Use this command to allow the switch to accept VLAN assignment by the RADIUS server.

**Default** disabled

**Format** `authorization network radius`

**Mode** Global Config

### *no authorization network radius*

Use this command to prohibit the switch from accepting VLAN assignment by the RADIUS server.

**Format** `authorization network radius`

**Mode** Global Config

## *show radius*

This command is used to display the various RADIUS configuration items for the switch as well as the configured RADIUS servers. If the optional token 'servers' is not included, the following RADIUS configuration items are displayed.

**Format** `show radius` *`[servers]`*

**Mode** Privileged EXEC

**Primary Server IP Address** The configured server currently in use for authentication.

**Number of configured servers** The configured IP address of the authentication server.

**Max number of retransmits** The configured value of the maximum number of times a request packet is retransmitted.

**Timeout Duration** The configured timeout value, in seconds, for request re-transmissions.

**Accounting Mode** Yes or No.

If you use the *`[servers]`* keyword, the following information displays:

**IP Address** IP address of the configured RADIUS server.

**Port** The port in use by this server.

**Type** Primary or secondary.

**Secret Configured** Yes / No.

**Message Authenticator** The message authenticator attribute for the selected server, which can be enables or disables.

## show radius accounting

This command is used to display the configured RADIUS accounting mode, accounting server and the statistics for the configured accounting server.

**Format** `show radius accounting [statistics <ipaddr>]`

**Mode** Privileged EXEC

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

**Mode** Enabled or disabled

**IP Address** The configured IP address of the RADIUS accounting server.

**Port** The port in use by the RADIUS accounting server.

**Secret Configured** Yes or No.

If you use the optional *statistics <ipaddr>* parameter, the statistics for the configured RADIUS accounting server are displayed. The IP address parameter must match that of a previously configured RADIUS accounting server. The following information regarding the statistics of the RADIUS accounting server is displayed.

**Accounting Server IP Address** IP address of the configured RADIUS accounting server

**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 the RADIUS accounting server.

**Requests** The number of RADIUS Accounting-Request packets sent to this accounting 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 and 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.

## show radius statistics

This command is used to display the statistics for RADIUS or configured server. To show the configured RADIUS server statistic, the IP address specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

**Format** `show radius statistics` *[<ipaddr>]*

**Mode** Privileged EXEC

If you do not specify the IP address, then only Invalid Server Address field is displayed. Otherwise other listed fields are displayed.

**Invalid Server Addresses** The number of RADIUS Access-Response packets received from unknown addresses.

**Server IP Address** IP address of the Server.

**Round Trip Time** The time interval, in hundredths of a second, between the most recent Access-Reply, Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.

**Access Requests** The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.

**Access Retransmission** 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, which were received from this server.

**Access Rejects** The number of RADIUS Access-Reject packets, including both valid and invalid packets, which were received from this server.

**Access Challenges** The number of RADIUS Access-Challenge packets, including both valid and invalid packets, which 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 RADIUS packets of unknown types, which 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.

# 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>* parameter is the IP address of the TACACS+ server. To specify multiple hosts, multiple **tacacs-server host** commands can be used.

**Format** **tacacs-server host** *<ip-address>*

**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>* parameter is the IP address of the TACACS+ server.

**Format** **no tacacs-server host** *<ip-address>*

**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.

**Format** **tacacs-server key** *<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).

**Format** **key** *<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>]*

**Mode** Privileged EXEC

**IP address** The IP address 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 267) to capture the running configuration into a script. Use the **copy** command (see "copy" on page 275) 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

**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

**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

# A

# List of Commands