D-Link®
Building Networks for People

DWS-1008
Release 2.0

# Wireless Switch

8 Port 10/100 Wireless Switch
With Power over Ethernet

# CLI Reference Guide

Business Class Networking

Download from Www.Somanuals.com. All Manuals Search And Download.

# Table of Contents


**Introducing the D-Link Mobility System ..... 1**
D-Link Mobility System ..... 1
**Using the Command-Line Interface ..... 2**
Text and Syntax: Conventions ..... 2
CLI Conventions ..... 3
Command Prompts ..... 3
Syntax: Notations ..... 4
Text Entry Conventions and Allowed Characters ..... 4
MAC Address Notation ..... 5
IP Address and Mask Notation ..... 5
Globs ..... 6
User Globs ..... 6
MAC Address Globs ..... 7
VLAN Globs ..... 7
Matching Order for Globs ..... 7
Port Lists ..... 8
Command-Line Editing ..... 9
Keyboard Shortcuts ..... 9
History Buffer ..... 9
Tabs ..... 9
Single-Asterisk (*) Wildcard Character ..... 10
Double-Asterisk (**) Wildcard Characters ..... 10
Using CLI Help ..... 10
Understanding Command Descriptions ..... 11
**Access Commands ..... 12**
**System Services Commands ..... 14**
**Port Commands ..... 33**
**VLAN Commands ..... 59**
**Quality of Service Commands ..... 73**
**IP Services Commands ..... 77**
**AAA Commands ..... 170**
**Cryptography Commands ..... 214**
**RADIUS and Server Groups Commands ..... 227**
**802.1X Management Commands ..... 240**
**Session Management Commands ..... 256**
**RF Detection Commands ..... 267**
**File Management Commands ..... 286**
**Access Point Commands ..... 307**
**STP Commands ..... 428**




Download from Www.Somanuals.com. All Manuals Search And Download.

**IGMP Snooping Commands .....450**
**Security ACL Commands.....469**
**Trace Commands.....490**
**Snoop Commands.....496**
**System Log Commands.....505**
**Boot Prompt Commands .....513**


Download from Www.Somanuals.com. All Manuals Search And Download.

# Introducing the D-Link Mobility System

Read this reference if you are a network administrator responsible for managing DWS-1008 switches and DWL-8220AP access points in a network.

# D-Link Mobility System

The D-Link Mobility System is an enterprise-class WLAN solution that seamlessly integrates with an existing wired enterprise network. The D-Link system provides secure connectivity to both wireless and wired users in large environments such as office buildings, hospitals, and university campuses and in small environments such as branch offices.

The D-Link Mobility System fulfills the three fundamental requirements of an enterprise WLAN: It eliminates the distinction between wired and wireless networks, allows users to work safely from anywhere (secure mobility), and provides a comprehensive suite of intuitive tools for planning and managing the network before and after deployment, greatly easing the operational burden on IT resources.

The D-Link Networks Mobility System consists of the following components:

- One or more DWS-1008 switches—Distributed, intelligent machines for managing user connectivity, connecting and powering Mobility Point access points, and connecting the WLAN to the wired network backbone.
- Multiple DWL-8220AP access points—Wireless access points (APs) that transmit and receive radio frequency (RF) signals to and from wireless users and connect them to a DWS-1008 switch.
- Mobility System Software™ —The operating system that runs all DWS switches and access points in a WLAN, and is accessible through a command-line interface (CLI) or the Web View interface. This software is built-in to the switch.


Download from Www.Somanuals.com. All Manuals Search And Download.

# Text and Syntax: Conventions

This CLI manual uses the following text and syntax conventions:

| Convention | Use |
|---|---|
| Monospace Text | Sets off command syntax or sample commands and system responses. |
| **Bold Text** | Highlights commands that you enter or items you select. |
| *Italic Text* | Designates command variables that you replace with appropriate values, or highlights publication titles or words requiring special emphasis. |
| Menu Name > Command | Indicates a menu item that you select. For example, **File** > **New** indicates that you select New from the File menu. |
| [ ] (square brackets) | Enclose optional parameters in command syntax. |
| { } (curly brackets) | Enclose mandatory parameters in command syntax. |
| \| (vertical bar) | Separates mutually exclusive options in command syntax. |

# Using the Command-Line Interface

The Mobility System Software (MMS) has a command-line interface (CLI) on the DWS-1008 switch that you can use to configure and manage the switch and its attached access points.

You configure the DWS switch and AP access points primarily with **set**, **clear**, and **show** commands. Use **set** commands to change parameters. Use **clear** commands to reset parameters to their defaults. In many cases, you can overwrite a parameter with another **set** command.

Use **show** commands to display the current configuration and monitor the status of network operations.


Download from Www.Somanuals.com. All Manuals Search And Download.

# CLI Conventions

Be aware of the following MSS CLI conventions for command entry:


- "Command Prompts" on page 3
- "Syntax: Notation" on page 4
- "Text Entry Conventions and Allowed Characters" on page 4
- "User Globs, MAC Address Globs, and VLAN Globs" on page 6
- "Port Lists" on page 8


## Command Prompts

By default, the MSS CLI provides the following prompt for restricted users. The *mmmm* portion shows the DWS switch model number (for example, 1008) and the *nnnnnn* portion shows the last 6 digits of the switch's media access control (MAC) address.

**DWS-mmmm-nnnnnn>**

After you become enabled as an administrative user by typing **enable** and supplying a suitable password, MSS displays the following prompt:

**DWS-mmmm-nnnnnn#**

For ease of presentation, this manual shows the restricted and enabled prompts as follows:

**DWS-1008>**
**DWS-1008#**

For information about changing the CLI prompt on an DWS switch, see **set prompt** on page 22.



Download from Www.Somanuals.com. All Manuals Search And Download.

# Syntax: Notations

The MSS CLI uses standard syntax notation:

- Bold monospace font identifies the command and keywords you must type. For example:

  **set enable pass**

- Italic monospace font indicates a placeholder for a value. For example, you replace vlan-id in the following command with a virtual LAN (VLAN) ID:

  **clear interface vlan-id ip**

- Curly brackets ({ }) indicate a mandatory parameter, and square brackets ([ ]) indicate an optional parameter. For example, you must enter dynamic or port and a port list in the following command, but a VLAN ID is optional:

  **clear fdb {dynamic l port port-list} [v1 an vlan-id]**

- A vertical bar (l) separates mutually exclusive options within a list of possibilities. For example, you enter either enable or disable, not both, in the following command:

  **set port {enable l disable} port-list**

# Text Entry Conventions and Allowed Characters

Unless otherwise indicated, the MSS CLI accepts standard ASCII alphanumeric characters, except for tabs and spaces, and is case-insensitive.

The CLI has specific notation requirements for MAC addresses, IP addresses, and masks, and allows you to group usernames, MAC addresses, virtual LAN (VLAN) names, and ports in a single command.

D-Link recommends that you do not use the same name with different capitalizations for VLANs or access control lists (ACLs). For example, do not configure two separate VLANs with the names red and RED.

The CLI does not support the use of special characters including the following in any named elements such as SSIDs and VLANs: ampersand (&), angle brackets (< >), number sign (#), question mark (?), or quotation marks (“ “).

In addition, the CLI does not support the use of international characters such as the accented E (é) in “décor”.


Download from Www.Somanuals.com. All Manuals Search And Download.

# MAC Address Notation

MSS displays MAC addresses in hexadecimal numbers with a colon (:) delimiter between bytes—for example, 00:01:02:1a:00:01. You can enter MAC addresses with either hyphen (-) or colon (:) delimiters, but colons are preferred.

For shortcuts:

- You can exclude leading zeros when typing a MAC address. MSS displays of MAC addresses include all leading zeros.
- In some specified commands, you can use the single-asterisk (*) wildcard character to represent from 1 byte to 5 bytes of a MAC address. (For more information, see “MAC Address Globs” on page 7.)

# IP Address and Mask Notation

MSS displays IP addresses in dotted decimal notation—for example, 192.168.1.11 MSS makes use of both subnet masks and wildcard masks.

**Subnet Masks**

Unless otherwise noted, use classless interdomain routing (CIDR) format to express subnet masks—for example, 192.168.1.112/24. You indicate the subnet mask with a forward slash (/) and specify the number of bits in the mask.

**Wildcard Masks**

Security access control lists (ACLs) use source and destination IP addresses and wildcard masks to determine whether the DWS switch filters or forwards IP packets. Matching packets are either permitted or denied network access. The ACL checks the bits in IP addresses that correspond to any Os (zeros) in the mask, but does not check the bits that correspond to Is (ones) in the mask. You specify the wildcard mask in dotted decimal notation.

For example, the address 10.0.0.0 and mask 0.255.255.255 match all IP addresses that begin with 10 in the first octet.

The ACL mask must be a contiguous set of zeroes starting from the first bit. For example, 0.255.255.255, 0.0.255.255, and 0.0.0.255 are valid ACL masks. However, 0.255.0.255 is not a valid ACL mask.


Download from Www.Somanuals.com. All Manuals Search And Download.

# Globs

Name “globbing” is a way of using a wildcard pattern to expand a single element into a list of elements that match the pattern. MSS accepts user globs, MAC address globs, and VLAN globs. The order in which globs appear in the configuration is important, because once a glob is matched, processing stops on the list of globs

## User Globs

A user glob is shorthand method for matching an authentication, authorization, and accounting (AAA) command to either a single user or a set of users.

A user glob can be up to 80 characters long and cannot contain spaces or tabs. The double-asterisk (**) wildcard characters with no delimiter characters match all usernames. The single-asterisk (*) wildcard character matches any number of characters up to, but not including, a delimiter character in the glob. Valid user glob delimiter characters are the at (@) sign and the period (.).

For example, the following globs identify the following users:

| User Glob | User(s) Designated |
|---|---|
| jose@example.com | User jose at example.com |
| *@example.com | All users at example.com whose usernames do not contain periods—for example, jose@example.com and tamara@example.com, but not nin.wong@example.com, because nin.wong contains a period. |
| *@marketing.example.com | All marketing users at example.com whose usernames do not contain periods. |
| * .*@marketing.example.com | All marketing users at example.com whose usernames contain a period. |
| * | All users with usernames that have no delimiters. |
| EXAMPLE* | All users in the Windows Domain EXAMPLE with usernames that have no delimiters. |
| EXAMPLE*.* | All users in the Windows Domain EXAMPLE whose usernames contain a period. |
| ** | All users |


Download from Www.Somanuals.com. All Manuals Search And Download.

# MAC Address Globs

A media access control (MAC) address glob is a similar method for matching some authentication, authorization, and accounting (AAA) and forwarding database (FDB) commands to one or more 6-byte MAC addresses. In a MAC address glob, you can use a single asterisk (*) as a wildcard to match all MAC addresses, or as follows to match from 1 byte to 5 bytes of the MAC address:

00:*
00: 01: *
00:01:02:*
00: 01: 02 : 03:*
00: 01: 02 : 03 : 04:*

For example, the MAC address glob 02:06:8c* represents all MAC addresses starting with 02:06:8c. Specifying only the first 3 bytes of a MAC address allows you to apply commands to MAC addresses based on an organizationally unique identity (OUI).

# VLAN Globs

A VLAN glob is a method for matching one of a set of local rules on a DWS-1008 switch, known as the location policy, to one or more users. MSS compares the VLAN glob, which can optionally contain wildcard characters, against the VLAN-Name attribute returned by AAA, to determine whether to apply the rule.

To match all VLANs, use the double-asterisk (**) wildcard characters with no delimiters. To match any number of characters up to, but not including, a delimiter character in the glob, use the single-asterisk (*) wildcard. Valid VLAN glob delimiter characters are the at (@) sign and the period (.).

For example, the VLAN glob bldg4. * matches bldg4.security and bldg4.hr and all other VLAN names with bldg4. at the beginning.

# Matching Order for Globs

In general, the order in which you enter AAA commands determines the order in which MSS matches the user, MAC address, or VLAN to a glob. To verify the order, view the output of the show aaa or show config command. MSS checks globs that appear higher in the list before items lower in the list and uses the first successful match.


Download from Www.Somanuals.com. All Manuals Search And Download.

# Port Lists

The physical Ethernet ports on a switch can be set for connection to access points, authenticated wired users, or the network backbone. You can include a single port or multiple ports in one MSS CLI command by using the appropriate list format.

The ports on a switch are numbered 1 through 8. No port 0 exists on the switch. You can include a single port or multiple ports in a command that includes **port** *port-list*. Use one of the following formats for port-list:

- A single port number. For example:

  DWS-1008# **set port enable 4**

- A comma-separated list of port numbers, with no spaces. For example:

  DWS-1008# **show port poe 1,2,4,6**

- A hyphen-separated range of port numbers, with no spaces. For example:

  DWS-1008# **reset port 1-4**

- Any combination of single numbers, lists, and ranges. Hyphens take precedence over commas. For example:

  DWS-1008# **show port status 1-3,6**


Download from Www.Somanuals.com. All Manuals Search And Download.

# Command-Line Editing

MSS editing functions are similar to those of many other network operating systems.

## Keyboard Shortcuts

The following keyboard shortcuts are available for entering and editing CLI commands:

| Keyboard Shortcut(s) | Function |
|---|---|
| Ctrl+A | Jumps to the first character of the command line. |
| Ctrl+B or Left Arrow key | Moves the cursor back one character. |
| Ctrl+C | Escapes and terminates prompts and tasks. |
| Ctrl+D | Deletes the character at the cursor. |
| Ctrl+E | Jumps to the end of the current command line. |
| Ctrl+F or Right Arrow key | Moves the cursor forward one character. |
| Ctrl+K | Deletes from the cursor to the end of the command line. |
| Ctrl+L or Ctrl+R | Repeats the current command line on a new line. |
| Ctrl+N or Down Arrow key | Enters the next command line in the history buffer. |
| Ctrl+P or Up Arrow key | Enters the previous command line in the history buffer. |
| Ctrl+U or Ctrl+X | Deletes characters from the cursor to the beginning of the command line. |
| Ctrl+W | Deletes the last word typed. |
| Esc B | Moves the cursor back one word. |
| Esc D | Deletes characters from the cursor forward to the end of the word. |
| Delete key or Backspace key | Erases mistake made during command entry. Reenter the command after using this key. |

## History Buffer

The history buffer stores the last 63 commands you entered during a terminal session. You can use the Up Arrow and Down Arrow keys to select a command that you want to repeat from the history buffer.

## Tabs

The MSS CLI uses the Tab key for command completion. You can type the first few characters of a command and press the Tab key to display the command(s) that begin with those characters.



Download from Www.Somanuals.com. All Manuals Search And Download.

# Single-Asterisk (*) Wildcard Character

You can use the single-asterisk (*) wildcard character in globbing. For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 7.

# Double-Asterisk (**) Wildcard Characters

The double-asterisk (**) wildcard character matches all usernames. For details, see “User Globs” on page 6.

# Using CLI Help

The CLI provides online help. To see the full range of commands available at your access level, type the following command:

```
DWS-1008# help
Commands:  ----------------------------------------------------------------------------------------------
clear        Clear, use ‘clear help’ for more information
commit       Commit the content of the ACL table
copy         Copy from filename (or url) to filename (or url)
crypto       Crypto, use ‘crypto help’ for more information
delete       Delete url
dir          Show list of files on flash device
disable      Disable privileged mode
exit         Exit from the Admin session
help         Show this help screen
history      Show contents of history substitution buffer
load         Load, use ‘load help’ for more information
logout       Exit from the Admin session
monitor      Monitor, use ‘monitor help’ for more information
ping         Send echo packets to hosts
quit         Exit from the Admin session
reset        Reset, use ‘reset help’ for more information
rollback     Remove changes to the edited ACL table
save         Save the running configuration to persistent storage
set          Set, use ‘set help’ for more information
show         Show, use ‘show help’ for more information
telnet       telnet IP address [server port]
traceroute   Print the route packets take to network host
```

To see a subset of the online help, type the command for which you want more information.


Download from Www.Somanuals.com. All Manuals Search And Download.

# Understanding Command Descriptions

Each command description in the D-Link Command Reference contains the following elements:

- A command name, which shows the keywords but not the variables. For example, the following command name appears at the top of a command description and in the index:

**set** {**ap** | **dap**} **name**

The **set** {**ap** | **dap**} **name** command has the following complete syntax:

**set** {**ap** *port-list* | **dap** *dap-num*} **name** *name*

- A brief description of the command's functions.
- The full command syntax.
- Any command defaults.
- The command access, which is either *enabled* or *all*.

  *All* indicates that anyone can access this command.

  *Enabled* indicates that you must enter the enable password before entering the command.

- The command history, which identifies the MSS version in which the command was introduced and the version numbers of any subsequent updates.


Download from Www.Somanuals.com. All Manuals Search And Download.

# Access Commands

Use access commands to control access to the Mobility Software System (MSS) (CLI). This chapter presents access commands alphabetically. Use the following table to locate commands in this chapter based on their use.

## disable

**Defaults:** None.

**Access:** Enabled.

## enable

Places the CLI session in enabled mode, which provides access to all commands required for configuring and monitoring the system.

**Syntax: enable**

**Access:** All.

**Usage:** MSS displays a password prompt to challenge you with the enable password. To enable a session, your or another administrator must have configured the enable password to this switch with the **set enablepass** command.

**Examples:** The following command plus the enable password provides enabled access to the CLI for the current sessions:

DWS-1008> **enable**

Enter **password**: *password*
DWS-1008#


Download from Www.Somanuals.com. All Manuals Search And Download.

# quit

Exit from the CLI session.

**Syntax: quit**

**Defaults:** None.

**Access:** All.

**Examples:** To end the administrator's session, type the following command:

DWS-1008> **quit**

# set enablepass

Sets the password that provides enabled access (for configuration and monitoring) to the switch.

**Syntax: set enablepass**

**Defaults:** None.

**Access:** Enabled.

**Usage:** After typing the **set enablepass** command, press **Enter**. If you are entering the first enable password on this switch, press **Enter** at the Enter old password prompt. Otherwise, type the old password. Then type a password of up to 32 alphanumeric characters with no spaces, and reenter it at the retype new password prompt.

**Examples:** The following example illustrates the prompts that the system displays when the enable password is changed. The passwords you enter are not displayed.

DWS-1008# **set enablepass**

**Enter old password:** *old-password*
**Enter new password:** *new-password*
**Retype new password:** *new-password*
Password changed


Download from Www.Somanuals.com. All Manuals Search And Download.

# System Services Commands

Use system services commands to configure and monitor system information for a DWS-1008 switch. This chapter presents system services commands alphabetically. Use the following table to located commands in this chapter based on their use.

| | |
|---|---|
| **Configuration** | quickstart on page 18 |
| **Auto-Config** | set auto-config on page 27 |
| **Display** | clear banner motd on page 15<br>set banner motd on page 19<br>show banner motd on page 28<br>set confirm on page 20<br>set length on page 20 |
| **System Identification** | set prompt on page 22<br>set system name on page 27<br>set system location on page 27<br>set system contact on page 23<br>set system countrycode on page 23<br>set system idle-timeout on page 25<br>set system ip-address on page 26<br>show load on page 29<br>show system on page 30<br>clear system on page 16<br>clear prompt on page 15 |
| **Help** | help on page 17 |
| **History** | history on page 18<br>clear history on page 15 |
| **License** | set license on page 21<br>show licenses on page 29 |
| **Technical Support** | show tech-support on page 32 |


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear banner motd

**Syntax: clear banner motd**

**Defaults:** None.

**Access:** Enabled.

**Examples:** To clear a banner, type the following command:

```
DWS-1008> clear banner motd
success: change accepted
```

**Note:** As an alternative to clearing the banner, you can overwrite the existing banner with an empty banner by typing the following command:

**set banner motd ^^**

# clear history

Deletes the command history buffer for the current CLI session.

**Syntax: clear history**

**Defaults:** None.

**Access:** All.

**Examples:** To clear the history buffer, type the following command:

```
DWS-1008# clear history
success: command buffer was flushed.
```

# clear prompt

**Syntax: clear prompt**

**Defaults:** None.

**Access:** Enabled.

**Examples:** To reset the prompt, type the following command:

```
wildebeest# clear prompt
success: change accepted.
DWS-1008#
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear system

Clears the system configuration of the specified information.

**Syntax: clear system [contact | countrycode | idle-timeout | ip-address | location | name]**

| | |
|---|---|
| **contact** | Resets the name of contact person for the DWS-1008 switch to null. |
| **countrycode** | Resets the country code for the DWS-1008 switch to null. |
| **idle-timeout** | Resets the number of seconds a CLI management session can remain idle to the default value (3600 seconds). |
| **ip-address** | Resets the IP address of the DWS-1008 switch to null. |
| **location** | Resets the location of the DWS-1008 switch to null. |
| **name** | Resets the name of the DWS-1008 switch to the default system name, which is DWS-mmmm-nnnnnn, where mmmm is the model number and nnnnnn is the last 6 digits of the switch's MAC address. |

**Defaults:** None.

**Access:** All.

**Examples:** To clear the location of the switch, type the following command:

```
DWS-1008# clear system location
success: change accepted
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# help

**Syntax: clear history**

**Defaults:** None.

**Access:** All.

**Examples:** Use this command to see a list of available commands. If you have restricted access, you see fewer commands than if you have enabled access. To display a list of CLI commands available at the enabled access level, type the following command at the enabled access level:

```
DWS-1008# help
Commands:
--------------------------------------------------------------------------------
clear                   Clear,  use 'clear help' for more information
commit                  Commit the content of the ACL table
copy                    Copy from filename (or url) to filename (or url)
crypto                  Crypto, use 'crypto help' for more information
delete                  Delete url
dir                     Show list of files on flash device
disable                 Disable privileged mode
exit                    Exit from the Admin session
help                    Show this help screen
history                 Show contents of history substitution buffer
hit-sample-rate         Set NP hit-counter sample rate
load                    Load, use 'load help' for more information
logout                  Exit from the Admin session
monitor                 Monitor, use 'monitor help' for more information
ping                    Send echo packets to hosts
quit                    Exit from the Admin session
reset                   Reset, use 'reset help' for more information
rollback                Remove changes to the edited ACL table
save                    Save the running configuration to persistent storage
set                     Set, use 'set help' for more information
show                    Show, use 'show help' for more information
telnet                  telnet IP address [server port]
traceroute              Print the route packets take to network host
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# history

**Syntax: clear history**

**Defaults:** None.

**Access:** All.

**Examples:** To show the history of your session, type the following command:

DWS-1008# **history**

```
Show History (most recent first)
--------------------------------
[00] show config
[01] show version
[02] enable
```

# quickstart

Runs a script that interactively helps you configure a new switch.

**Caution!** The **quickstart** command is for configuration of a new switch only. After prompting you for verification, the command erases the switch's configuration before continuing. If you run this command on a switch that already has a configuration, the configuration will be erased. In addition, error messages such as *Critical AP Notice* for directly connected APs can appear.


Download from Www.Somanuals.com. All Manuals Search And Download.

# set banner motd

Configures the banner string that is displayed before the beginning of each login prompt for each CLI session on the DWS-1008 switch.

**Syntax: set banner motd** *^text^*

**Defaults:** None.

**Access:** Enabled.

**Usage:** Type a caret (^), then the message, then another caret.

Do not use the following characters with commands in which you set text to be displayed on the DWS-1008 switch, such as message-of-the-day (MOTD) banners:

- Ampersand (&)
- Angle brackets (< >)
- Double quotation marks (“ ”)
- Number sign (#)
- Question mark (?)
- Single quotation mark (‘)

**Examples:** To create a banner that says *Update meeting at 3 p.m.*, type the following command:

```
DWS-1008> set banner motd ^Update meeting at 3 p.m.^
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set confirm

Enables or disables the display of confirmation messages for commands that might have a large impact on the network.

**Syntax: set confirm {on | off}**

**on** Enables confirmation messages.

**off** Disables confirmation messages.

**Defaults:** Configuration messages are enabled.

**Access:** Enabled.

**Usage:** This command remains in effect for the duration of the session, until you enter an **exit** or **quit** command, or until you enter another **set confirm** command.

MSS displays a message requiring confirmation when you enter certain commands that can have a potentially large impact on the network. For example:

```
DWS-1008# clear vlan red
This may disrupt user connectivity. Do you wish to continue? (y/n) [n]
```

**Examples:** To turn off these confirmation messages, type the following command:

```
DWS-1008# set confirm off
success: Confirm state is off
```

# set length

Defines the number of lines of CLI output to display between paging prompts. MSS displays the set number of lines and waits for you to press any key to display another set, or type **q** to quit the display.

**Syntax: set length** *number-of-lines*

*number-of-lines* Number of lines of text to display between paging prompts. You can specify from 0 to 512. The 0 value disables the paging prompt action entirely.

**Defaults:** MSS displays 24 lines by default.

**Access:** All.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** Use this command if the output of a CLI command is greater than the number of lines allowed by default for a terminal type.

**Examples:** To set the number of lines displayed to 100, type the following command:

```
DWS-1008# set length 100
success: screen length for this session set to 100
```

# set license

Installs an upgrade license key on a DWS-1008 switch.

The DWS-1008 can boot and manage up to 32 APs by default. You can increase the AP support to 64, 96, or 128 APs, by installing one or more activation keys. You can install a 32-AP upgrade, 64-AP upgrade, or 96-AP upgrade. If you have already installed a 32-AP or 64-AP upgrade, you can still install additional upgrades.

**Syntax: set license** *activation-key*

| | |
|---|---|
| *activation-key* | Hexadecimal digits generated by the D-Link license server or otherwise provided by D-Link for your switch.<br><br>The activation key is based on the switch's serial number.<br>You can enter the number in either of the following formats:<br><br>xxxx-xxxx-xxxx-xxxx-xxxx<br>xxxxxxxxxxxxxxxxxxxx |

**Defaults:** None.

**Access:** Enabled.

**Usage:** This command applies to the DWS-1008.

**Examples:** To install an activation key for an additional 80 APs, type the following command:

```
DWS-1008# set license 3B02-D821-6C19-CE8B-F20E
success: license accepted
```

**See Also:**
- show licenses


Download from Www.Somanuals.com. All Manuals Search And Download.

# set prompt

Changes the CLI prompt for the DWS-1008 switch to a string you specify.

**Syntax: set prompt** *string*

| | |
|---|---|
| *string* | Alphanumeric string up to 32 characters long. To include spaces in the prompt, you must enclose the string in double quotation marks (“”). |

**Defaults:** The factory default for the DWS switch prompt is DWS-mm-nnnnnn, where mm is the model number and nnnnnn is the last 6 digits of the 12-digit system MAC address.

**Access:** Enabled.

**Usage:** When you first log in for the initial configuration of the DWS switch, the CLI provides an DWS-*mmmm-nnnnnn*> prompt. After you become enabled by typing enable and giving a suitable password, the DWS-*mmmm-nnnnnn#* prompt is displayed.

If you use the **set system name** command to change the default system name, MSS uses that name in the prompt, unless you also change the prompt with **set prompt**.

**Examples:** The following example sets the prompt from DWS to *happy_days*:

```
DWS-1008# set prompt happy_days
success: change accepted.
happy_days#
```

**See Also:**
- clear prompt
- set system name
- show config


Download from Www.Somanuals.com. All Manuals Search And Download.

# set system contact

Stores a contact name for the DWS-1008 switch.

**Syntax: set system contact** *string*

*string* Alphanumeric string up to 256 characters long, with no blank spaces.

**Defaults:** None.

**Access:** Enabled.

To view the system contact string, type the **show system** command.

**Examples:** The following command sets the system contact information to *tamara@example.com*:

```
DWS-1008# set system contact tamara@example.com
success: change accepted.
```

**See Also:**

- clear system
- set system location
- set system name
- show system

# set system country code

Defines the country-specific IEEE 802.11 regulations to enforce on the DWS-1008 switch.

**Syntax: set system countrycode** *code*

*code* Two-letter code for the country of operation for the DWS switch. You can specify one of the codes listed in the table below


Download from Www.Somanuals.com. All Manuals Search And Download.

**Country Codes**

| Country | Code |
|---|---|
| Australia | **AU** |
| Austria | **AT** |
| Belgium | **BE** |
| Brazil | **BR** |
| Canada | **CA** |
| China | **CN** |
| Czech Republic | **CZ** |
| Denmark | **DK** |
| Finland | **FI** |
| France | **FR** |
| Germany | **DE** |
| Greece | **GR** |
| Hong Kong | **HK** |
| Hungary | **HU** |
| Iceland | **IS** |
| India | **IN** |
| Ireland | **IE** |
| Israel | **IL** |
| Italy | **IT** |
| Japan | **JP** |
| Liechtenstein | **LI** |
| Luxembourg | **LU** |
| Malaysia | **MY** |
| Mexico | **MX** |
| Netherlands | **NL** |
| New Zealand | **NZ** |
| Norway | **NO** |
| Poland | **PL** |
| Portugal | **PT** |
| Saudi Arabia | **SA** |
| Singapore | **SG** |
| Slovakia | **SK** |
| Slovenia | **SI** |
| South Africa | **ZA** |
| South Korea | **KR** |
| Spain | **ES** |
| Sweden | **SE** |
| Switzerland | **CH** |
| Taiwan | **TW** |
| Thailand | **TH** |
| United Arab Emirates | **AE** |
| United Kingdom | **GB** |
| United States | **US** |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** Enabled.

**Usage:** You must set the system county code to a valid value before using any **set ap** commands to configure an access point.

**Examples:** To set the country code to Canada, type the following command:

```
DWS-1008# set system country code CA
success: change accepted.
```

**See Also:**
- show config

# set system idle-timeout

Specifies the maximum number of seconds a CLI management session with the switch can remain idle before MSS terminates the session.

**Syntax: set system idle-timeout** *seconds*

*seconds* Number of seconds a CLI management session can remain idle before MSS terminates the session. You can specify from 0 to 86400 seconds (one day). If you specify 0, the idle timeout is disabled.

The timeout interval is in 30-second increments. For example, the interval can be 0, or 30 seconds, or 60 seconds, or 90 seconds, and so on. If you enter an interval that is not divisible by 30, the CLI rounds up to the next 30-second increment. For example, if you enter 31, the CLI rounds up to 60.

**Defaults:** 3600 seconds (one hour).


Download from Www.Somanuals.com. All Manuals Search And Download.

**Access:** Enabled.

**Usage:** This command applies to all types of CLI management sessions: console, Telnet, and SSH. The timeout change applies to existing sessions only, not to new sessions.

**Examples:** The following command sets the idle timeout to 1800 seconds (one half hour):

```
DWS-1008# set system idle-timeout 1800
success: change accepted.
```

**See Also:**
- clear system
- show system

# set system ip-address

Sets the system IP address so that it can be used by various services in the DWS-1008 switch.

**Syntax: set system ip-address** *ip-addr*

*ip-addr* IP address, in dotted decimal notation.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command sets the IP address of the DWS switch to 192.168.253.1:

```
DWS-1008# set system ip-address 192.168.253.1
success: change accepted.
```

**See Also:**
- clear system
- set interface
- show system


Download from Www.Somanuals.com. All Manuals Search And Download.

# set system location

Stores location information for the DWS-1008 switch.

**Syntax: set system location** *string*

*string* Alphanumeric string up to 256 characters long, with no blank spaces.

**Defaults:** None.

**Access:** Enabled.

To view the system location string, type the **show system** command.

**Examples:** To store the location of the switch in the switch's configuration, type the following command:

```
DWS-1008# set system location first-floor-bldg3
success: change accepted.
```

**See Also:**
- clear system
- set system contact
- set system name
- show system

# set system name

Changes the name of the switch from the default system name and also provides content for the CLI prompt, if you do not specify a prompt.

**Syntax: set system name** *string*

*string* Alphanumeric string up to 256 characters long, with no blank spaces.

**Defaults:** By default, the system name and command prompt have the same value. The factory default for both is DWS-*mmmm-nnnnnn*, where *mmmm* is the model number and *nnnnnn* is the last 6 digits of the 12-digit system MAC address.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** Entering set system name with no string resets the system name to the factory default.

To view the system name string, type the **show system** command.

**Examples:** The following example sets the system name to a name that identifies the DWS switch:

```
DWS-1008# set system name DWS-bldg3
success: change accepted.
DWS-1008-bldg3#
```

**See Also:**
- clear system
- set prompt
- set system contact
- set system location
- show system

## show banner motd

Shows the banner that was configured with the **set banner motd** command.

**Syntax: show banner motd**

**Defaults:** None.

**Access:** Enabled.

**Examples:** To display the banner with the message of the day, type the following command:

```
DWS-1008# show banner motd
hello world
```

**See Also:**
- clear banner motd


Download from Www.Somanuals.com. All Manuals Search And Download.

# show licenses

Displays information about the license key(s) currently installed on an DWS-1008 switch.

**Syntax: show licenses**

**Defaults:** None.

**Access:** All

**Examples:** To view license keys, type the following command:

```
DWS-1008# show licenses
Feature         : 80 additional APs
```

**See Also:**
• set license

# show load

Displays CPU usage on a DWS-1008 switch.

**Syntax: show load**

**Defaults:** None.

**Access:** Enabled.

**Examples:** To display the CPU load recorded from the time the switch was booted, as well as from the previous time the show load command was run, type the following command:

```
DWS-1008# show load
System Load: overall: 2% delta: 5%
```

The overall field shows the CPU load as a percentage from the time the switch was booted. The delta field shows CPU load as a percentage from the last time the **show load** command was entered.


Download from Www.Somanuals.com. All Manuals Search And Download.

# show system

Displays system information.

**Syntax: show system**

**Defaults:** None.

**Access:** Enabled.

**Examples:** To show system information, type the following command:

DWS-1008# **show system**

```
================================================================================
 Product Name:       DWS-1008
 System Name:        DWS-bldg3
 System Countrycode: US
 System Location:    first-floor-bldg3
 System Contact:     tamara@example.com
 System IP:          192.168.12.7
 System idle timeout:3600
 System MAC:         00:0B:0E:00:04:30
================================================================================
 Boot Time:          2003-11-07 15:45:49
 Uptime:                 13 days 04:29:10
================================================================================
 Fan status:  fan1 OK fan2 OK fan3 OK
 Temperature: temp1 ok  temp2 ok  temp3 ok
 PSU Status:  Lower Power Supply DC ok AC ok  Upper Power Supply missing
 Memory:      97.04/744.03 (13%)
 Total Power Over Ethernet : 29.000
================================================================================
```

The table on the next page describes the fields of **show system** output.


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| Product Name | DWS model number. |
| System Name | System name (factory default, or optionally configured with **set system name**). |
| System Countrycode | Country-specific 802.11 code required for AP operation. (configured with **set system countrycode**) |
| Total Power Over Ethernet | Total power that the DWS-1008 is currently supplying to its directly connected access points, in watts. |
| System Location | Record of the DWS switch's physical location (optionally configured with **set system location**). |
| System Contact | Contact information about the system administrator or another person to contact about the system (optionally configured with **set system contact**). |
| System IP | Common interface, source, and default IP address for the DWS-1008, in dotted decimal notation (configured with **set system ip-address**). |
| System idle timeout | Number of seconds MSS allows a CLI management session (console, Telnet, or SSH) to remain idle before terminating the session. (The system idle timeout can be configured using the **set system idle-timeout** command.) |
| System MAC | DWS-1008 media access control (MAC) machine address set at the factory, in 6-byte hexadecimal format. |
| Boot Time | Date and time of the last system reboot. |
| Uptime | Number of days, hours, minutes, and seconds that the switch has been operating since its last restart. |
| Fan status | Operating status of the three switch cooling fans:<br>• OK—Fan is operating.<br>• Failed—Fan is not operating. MSS sends an alert to the system log every 5 minutes until this condition is corrected. Fan 1 is located nearest the front of the chassis, and fan 3 is located nearest the back. |
| Temperature | Status of temperature sensors at three locations in the DWS-1008 switch:<br>• ok—Temperature is within the acceptable range of 0° C to 50° C (32° F to 122° F).<br>• Alarm—Temperature is above or below the acceptable range. MSS sends an alert to the system log every 5 minutes until this condition is corrected. |
| PSU Status | Status of the lower and upper power supply units:<br>• missing—Power supply is not installed or is inoperable.<br>• DC ok—Power supply is producing DC power.<br>• DC output failure—Power supply is not producing DC power. MSS sends an alert to the system log every 5 minutes until this condition is corrected.<br>• AC ok—Power supply is receiving AC power.<br>• AC not present—Power supply is not receiving AC power. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| Memory | Current size (in megabytes) of nonvolatile memory (NVRAM) and synchronous dynamic RAM (SDRAM), plus the percentage of total memory space in use, in the following format:<br>*NVRAM size /SDRAM size (percent of total)* |
| Total Power Over Ethernet | Total power that the DWS-1008 is currently supplying to its directly connected access points, in watts. |

**See Also:**
- clear system
- set system contact
- set system countrycode
- set system idle-timeout
- set system ip-address
- set system location
- show system name

# show tech-support

Provides an in-depth snapshot of the status of the DWS switch, which includes details about the boot image, the version, ports, and other configuration values. This command also displays the last 100 log messages.

**Syntax: show tech-support [file [***subdirname/***] *filename***]**

| | |
|---|---|
| *[subdirname/]filename* | Optional subdirectory name, and a string up to 32 alphanumeric characters. The command's output is saved into a file with the specified name in nonvolatile storage. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** Enter this command before calling D-Link Technical Support.

**Examples:** To store the location of the DWS-1008 switch in the switch's configuration, type the following command:

```
DWS-1008# set system location first-floor-bldg3
success: change accepted.
```

**See Also:**
- show boot
- show config
- set licenses


Download from Www.Somanuals.com. All Manuals Search And Download.

# Port Commands

Use port commands to configure and manage individual ports and load-sharing port groups. This chapter presents port commands alphabetically. Use the following table to locate commands in this chapter based on their use.

| | |
|---|---|
| **Port Type** | set port type ap on page 51<br>set dap on page 42<br>set port type wired-auth on page 53<br>clear dap on page 34<br>clear port type on page 36<br>show port status on page 58 |
| **Name** | set port name on page 46<br>clear port name on page 36 |
| **State** | set port on page 43<br>reset port on page 42 |
| **Interface Type** | set port media-type on page 35<br>clear port media-type on page 36 |
| **Speed** | set port speed on page 49 |
| **Autonegotiation** | set port negotiation on page 47 |
| **PoE** | set port poe on page 48<br>show port poe on page 57 |
| **SNMP** | set port trap on page 50 |
| **Port Groups** | set port-group on page 44 |
| **Port Mirroring** | clear port-group on page 35<br>set port mirror on page 46 |
| **Statistics** | clear port mirror on page 35<br>show port counters on page 58<br>monitor port counters on page 38<br>clear port counters on page 34 |


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear dap

**Caution:** When you clear a Distributed AP, MSS ends user sessions that are using the AP.

Removes a Distributed AP.

**Syntax: clear dap** *dap-num*

*dap-num* Number of the Distributed AP(s) you want to remove.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command clears Distributed AP 1:

```
DWS-1008# clear dap 1
This will clear specified DAP devices. Would you like to continue? (y/n)
[n]y
```

**See Also:**
- set dap
- set port type ap

# clear port counters

Clears port statistics counters and resets them to 0.

**Syntax: clear port counters**

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command clears all port statistics counters and resets them to 0:

```
DWS-1008# clear port counters
success: cleared port counters
```

**See Also:**
- monitor port counters
- set port counters


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear port-group

Removes a port group

**Syntax: clear port-group name** *name*

*name* Name of the port group.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command clears port group server1:

```
DWS-1008# clear port-group name server1
success: change accepted.
```

**See Also:**
• set port-group

# clear port mirror

Removes a port mirroring configuration.

**Syntax: clear port mirror**

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command clears the port mirroring configuration from the switch:

```
DWS-1008# clear port mirror
```

**See Also:**
• set port mirror


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear port name

Removes the name assigned to a port.

**Syntax: clear port** *port-list* **name**

| | |
|---|---|
| *port-list* | List of physical ports. MSS removes the names from all the specified ports. |

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command clears the names of ports 1 through 4:

DWS-1008# **clear port 1-4 name**

**See Also:**
• set port name

# clear port type

**Caution:** When you clear a port, MSS ends user sessions that are using the port.

Removes all configuration settings from a port and resets the port as a network port.

**Syntax: clear port type** *port-list*

| | |
|---|---|
| *port-list* | List of physical ports. MSS resets and removes the configuration from all the specified ports. |

**Defaults:** The cleared port becomes a network port but is not placed in any VLANs.

**Access:** Enabled.

**Usage:** Use this command to change a port back to a network port. All configuration settings specific to the port type are removed. For example, if you clear an access point port, all AP-specific settings are removed. The following table lists the default network port settings that MSS applies when you clear a port's type:


Download from Www.Somanuals.com. All Manuals Search And Download.

| Port Parameter | Setting |
|---|---|
| VLAN membership | None.<br><br>**Note:** Although the command changes a port to a network port, the command does not place the port in any VLAN. To use the port in a VLAN, you must add the port to the VLAN. |
| Spanning Tree Protocol (STP) | Based on the VLAN(s) you add the port to. |
| 802.1X | No authorization. |
| Port groups | None. |
| Internet Group Management Protocol (IGMP) snooping | Enabled as port is added to VLANs. |
| Access: point and radio parameters | Not applicable. |
| Maximum user sessions | Not applicable. |

**Examples:** The following command clears port 5:

```
DWS-1008# clear port type 5
This may disrupt currently authenticated users. Are you sure? (y/n) [n]y
success: change accepted.
```

**See Also:**
- set port type ap
- set port type wired-auth


Download from Www.Somanuals.com. All Manuals Search And Download.

# monitor port counters

Displays and continually updates port statistics.

**Syntax: monitor port counters [octets | packets | receive-errors | transmit-errors | collisions | receive-etherstats | transmit-etherstats]**

| | |
|---|---|
| **octets** | Displays octet statistics first. |
| **packets** | Displays packet statistics first. |
| **recieve-errors** | Displays errors in received packets first. |
| **transmit-errors** | Displays errors in transmitted packets first. |
| **collisions** | Displays collision statistics first. |
| **receive-etherstats** | Displays Ethernet statistics for received packets first. |
| **transmit-etherstats** | Displays Ethernet statistics for transmitted packets first. |

**Defaults:** All types of statistics are displayed for all ports. MSS refreshes the statistics every 5 seconds. This interval cannot be configured. Statistics types are displayed in the following order by default:

- Octets
- Packets
- Receive errors
- Transmit errors
- Collisions
- Receive Ethernet statistics
- Transmit Ethernet statistics

**Access:** All.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** Each type of statistic is displayed separately. Press the Spacebar to cycle through the displays for each type.

If you use an option to specify a statistic type, the display begins with that statistic type. You can use one statistic option with the command.

Use the keys listed the following table to control the monitor display

| Key | Effect on monitor display |
|---|---|
| Spacebar | Advances to the next statistic type. |
| Esc | Exits the monitor. MSS stops displaying the statistics and displays a new command prompt. |
| c | Clears the statistics counters for the currently displayed statistics type. The counters begin incrementing again. |

For error reporting, the cyclic redundancy check (CRC) errors include misalignment errors. Jumbo packets with valid CRCs are not counted. A short packet can be reported as a short packet, a CRC error, or an overrun. In some circumstances, the transmitted octets counter might increment a small amount for a port with nothing attached.

**Examples:** The following command starts the port statistics monitor beginning with octet statistics (the default):

**Syntax: monitor port counters**

As soon as you press Enter, MSS clears the window and displays statistics at the top of the window**.**

```
Port  Status              Rx Octets          Tx Octets
=========================================
1     Up                  27965420           34886544
...
```

To cycle the display to the next set of statistics, press the Spacebar. In this example, packet statistics are displayed next:

```
Port  Status      Rx Unicast  Rx NonUnicast     Tx Unicast        Tx NonUnicast
=========================================================================
1     Up          54620       62144             58318             62556
...
```

The following table describes the port statistics displayed by each statistics option. The Port and Status fields are displayed for each option.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Table: Output for monitor port counters**

| Statistics Option | Field | Description |
|---|---|---|
| **Displayed for All Options** | Port | Port the statistics are displayed for. |
| | Status | Port status. The status can be Up or Down. |
| **octets** | Rx Octets | Total numbewr of octets reveived by the port.<br><br>This number includes octets received in frames that contained errors. |
| | Tx Octets | Total number of octets transmitted.<br><br>This number includes octets transmitted in frames that contained errors. |
| **packets** | Rx Unicast | Number of unicast packets received.<br><br>This number does not include packets that contain errors. |
| | Rx NonUnicast | Number of broadcast and multicast packets received.<br><br>This number does not include packets that contain errors. |
| | Tx Unicast | Number of unicast packets transmitted.<br><br>This number does not include packets that contain errors. |
| | Tx NonUnicast | Number of broadcast and multicast packets transmitted.<br><br>This number does not include packets that contain errors. |
| **receive-errors** | Rx Crc | Number of frames received by the port that had the correct length but contained an invalid frame check sequence (FCS) value. This statistic includes frames with misalignment errors. |
| | Rx Error | Total number of frames received in which the Physical layer (PHY) detected an error. |
| | Rx Short | Number of frames received by the port that were fewer than 64 bytes long. |
| | Rx Overrun | Number of frames received by the port that were valid but were longer than 1518 bytes.<br><br>This statistic does not include jumbo packets with valid CRCs. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Statistics Option | Field | Description |
|---|---|---|
| **Transmit-errors** | Tx Crc | Number of frames transmitted by the port that had the correct length but contained an invalid FCS value. |
| | Tx Short | Number of frames transmitted by the port that were fewer than 64 bytes long. |
| | Tx Fragment | Total number of frames transmitted that were less than 64 octets long and had invalid CRCs. |
| | Tx Abort | Total number of frames that had a link pointer parity error. |
| **collisions** | Single Coll | Total number of frames transmitted that experienced one collision before 64 bytes of the frame were transmitted on the network. |
| | Multiple Coll | Total number of frames transmitted that experienced more than 1 collision before 64 bytes of the frame were transmitted on the network. |
| | Excessive Coll | Total number of frames that experienced more than 16 collisions during transmit attempts. These frames are dropped and not transmitted. |
| | Total Coll | Best estimate of the total number of collisions on this Ethernet segment. |
| **receive-etherstats** | Rx 64 | Number of packets received that were 64 bytes long. |
| | Rx 127 | Number of packets received that were 65-127 bytes long. |
| | Rx 255 | Number of packets received that were 128-255 bytes long. |
| | Rx 511 | Number of packets received that were 256-511 bytes long. |
| | Rx 1023 | Number of packets received that were 512-1023 bytes long. |
| | Rx 1518 | Number of packets received that were 1024-1518 bytes long. |
| **transmit-etherstats** | Tx 64 | Number of packets transmitted that were 64 bytes long. |
| | Tx 127 | Number of packets transmitted that were 65-127 bytes long. |
| | Tx 255 | Number of packets transmitted that were 128-255 bytes long. |
| | Tx 511 | Number of packets transmitted that were 256-511 bytes long. |
| | Tx 1023 | Number of packets transmitted that were 512-1023 bytes long. |
| | Tx 1518 | Number of packets transmitted that were 1024-1518 bytes long. |


Download from Www.Somanuals.com. All Manuals Search And Download.

# reset port

Resets a port by toggling its link state and Power over Ethernet (PoE) state.

**Syntax: reset port** *port-list*

*port-list* List of physical ports. MSS resets all the specified ports.

**Defaults:** None.

**Access:** Enabled.

**Usage:** The reset command disables the port's link and PoE (if applicable) for at least 1 second, then reenables them. This behavior is useful for forcing an AP access point that is connected to two DWS-1008 switches to reboot over the link to the other switch.

**Examples:** The following command resets port 5:

```
DWS-1008# reset port 5
```

**See Also:**
• set port

# set dap

Configures a Distributed AP for an access point that is indirectly connected to the DWS-1008 switch through an intermediate Layer 2 or Layer 3 network.

**Note.** Before configuring a Distributed AP, you must use the set system countrycode command to set the IEEE 802.11 country-specific regulations on the DWS-1008 switch. See **set system countrycode**.

**Syntax: set dap** *dap-num* **serial-id** *serial-ID* **model {DWL-8220AP} [radiotype {11a | 11b| 11g}]**

*dap-num*
Number for the Distributed AP.

**serial id** *serial ID* AP access point serial ID. The serial ID is listed on the AP case. To display the serial ID using the CLI, use the **show version details** command.

**model**
AP access point model.

**Defaults:** The default vales are the same as the defaults for the **set port type ap** command.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Access:** Enabled.

**Examples:** The following command configures Distributed AP 1 for AP model MP-372 with serial-ID 0322199999:

```
DWS-1008# set dap 1 serial-id 0322199999 model mp-372
success: change accepted.
```

The following command removes Distributed AP 1:

```
DWS-1008# clear dap 1
This will clear specified DAP devices. Would you like to continue? (y/n)
[n]y
```

**See Also:**
- clear dap
- clear port type
- set port type ap
- set system countrycode

# set port

Administratively disables or reenables a port.

**Syntax: set port {enable | disable}** *port-list*

| | |
|---|---|
| **enable** | Enables the specified ports. |
| **disable** | Disables the specified ports. |
| *port-list* | List of physical ports. MSS disables or reenables all the specified ports. |

**Defaults:** All ports are enabled.

**Access:** Enabled.

**Usage:** A port that is administratively disabled cannot send or receive packets. This command does not affect the link state of the port.

**Examples:** The following command disables port 4:

```
DWS-1008# set port disable 4
success: set “disable” on port 4
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The following command reenables the port:

```
DWS-1008# set port enable 4
success: set “enable” on port 4
```

**See Also:**
• set reset port

# set port-group

Administratively disables or reenables a port.

**Syntax: set port-group name** *group-name port-list* **mode {on | off}**

| | |
|---|---|
| **name** *group-name* | Alphanumeric string of up to 255 characters, with no spaces. |
| *port-list* | List of physical ports. All the ports you specify are configured together as a single logical link. |
| **mode {on \| off}** | State of the group. Use **on** to enable the group or **off** to disable the group. The group is enabled by default. |

**Defaults:** Once configured, a group is enabled by default.

**Access:** Enabled.

**Usage:** Do not use dashes or hyphens in a port group name. If you do, MSS will not display or save the port group.

You can configure up to 8 ports in a port group, in any combination of ports. The port numbers do not need to be contiguous and you can use 10/100 Ethernet ports in the same port group.

After you add a port to a port group, you cannot configure port parameters on the individual port. Instead, change port parameters on the entire group. Specify the group name instead of an individual port name or number in port configuration commands.

To add or remove ports in a group that is already configured, change the mode to **off**, add or remove the ports, then change the mode to **on**.

**Examples:** The following command configures a port group named *server1* containing ports 1 through 5, and enables the link:

```
DWS-1008# port-group name server1 1-5 mode on
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The following commands disable the link for port group *server1*, change the list of ports in the group, and reenable the link:

DWS-1008# **set port-group name server1 1-5 mode off**
success: change accepted.

DWS-1008# **set port-group name server1 1-4,7 mode on**
success: change accepted.

**See Also:**

- clear port-group


Download from Www.Somanuals.com. All Manuals Search And Download.

# set port mirror

Configures port mirroring. Port mirroring is a troubleshooting feature that copies (mirrors) traffic sent or received by a DWS-1008 port (the source port) to another port (the observer) on the same DWS-1008. You can attach a protocol analyzer to the observer port to examine the source port's traffic. Both traffic directions (send and receive) are mirrored.

**Syntax: set port mirror** *source-port* **observer** *observer-port*

| | |
|---|---|
| *source-port* | Number of the port whose traffic you want to analyze. You can specify only one port. |
| *observer-port* | Number of the port to which you want the switch to copy the source port's traffic. |

**Defaults:** None

**Access:** Enabled.

**Usage:** The switch can have one port mirroring pair (one source port and one observer port) at a time. The source port can be a network port, AP access port, or wired authentication port. However, the observer port must be a network port, and cannot be a member of any VLAN or port group.

**Examples:** The following command sets port 2 to monitor port 1's traffic:

```
DWS-1008# set mirror port 1 observer 2
```

**See Also:**
• clear port mirror

# set port name

Assigns a name to a port. After naming a port, you can use the port name or number in other CLI commands.

**Syntax: set port** *port* **name** *name*

| | |
|---|---|
| *port* | Number of a physical port. You can specify only one port. |
| **name** *name* | Alphanumeric string of up to 16 characters, with no spaces. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None

**Access:** Enabled.

**Usage:** To simplify configuration and avoid confusion between a port's number and its name, D-Link recommends that you do not use numbers as port names.

**Examples:** The following command sets the name of port 4 to adminpool:

```
DWS-1008# set port 4 name adminpool
success: change accepted.
```

**See Also:**
• clear port name

# set port negotiation

Disables or reenables autonegotiation on gigabit Ethernet or 10/100 Ethernet ports.

**Syntax: set port negotiation** *port-list* **{enable | disable}**

| | |
|---|---|
| *port-list* | List of physical ports. MSS disables or reenablesautonegotiation on all the specified ports. |
| **enable** | Enables autonegotiation on the specified ports. |
| **disable** | Disables autonegotiation on the specified ports. |

**Defaults:** Autonegotiation is enabled on all Ethernet ports by default.

**Access:** Enabled.

**Usage:** The gigabit Ethernet ports operate at 1000 Mbps only. They do not change speed to match 10-Mbps or 100-Mbps links.

The DWS-1008 Ethernet ports support half-duplex and full-duplex operation.

D-Link recommends that you do not configure the mode of a DWS-1008 port so that one side of the link is set to autonegotiation while the other side is set to full-duplex. Although MSS allows this configuration, it can result in slow throughput on the link. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex.


Download from Www.Somanuals.com. All Manuals Search And Download.

A stream of large packets sent to an DWS-1008 port in such a configuration can cause forwarding on the link to stop.

**Examples:** The following command disables autonegotiation on ports 1, 2, and 4 through 6:

DWS-1008# **set port negotiation 1,2,4-6 disable**

The following command enables autonegotiation on port 5:

DWS-1008# **set port negotiation 5 enable**

# set port poe

Enables or disables Power over Ethernet (PoE) on ports connected to AP access points.

**Caution!** When you set the port type for AP use, you can enable PoE on the port. Use the DWS-1008's PoE to power D-Link access points or PoE enabled devices only. If you enable PoE on ports connected to other devices, damage can result.

**Syntax: set port poe** *port-list* **enable | disable**

| | |
|---|---|
| *port-list* | List of physical ports. MSS disables or reenables PoE on all the specified ports. |
| **enable** | Enables PoE on the specified ports. |
| **disable** | Disables PoE on the specified ports. |

**Defaults:** PoE is disabled on network and wired authentication ports. The state on access point ports depends on whether you enabled or disabled PoE when setting the port type. See **set port type ap**.

**Access:** Enabled.

**Usage:** This command does not apply to any gigabit Ethernet ports or to port 3 on the DWS-1008 switch.

**Examples:** The following command disables PoE on ports 3 and 5, which are connected to an access point:


Download from Www.Somanuals.com. All Manuals Search And Download.

DWS-1008# **set port poe 3,5 disable**
If you are enabling power on these ports, they must be connected only to approved PoE devices with the correct wiring. Do you wish to continue? (y/n) [n]y

The following command enables PoE on ports 2 and 4:

DWS-1008# **set port poe 2,4 enable**
If you are enabling power on these ports, they must be connected only to approved PoE devices with the correct wiring. Do you wish to continue? (y/n) [n]y

**See Also:**
- set port type ap
- set port type wired-auth

# set port speed

Changes the speed of a port.

**Syntax: set port speed** *port-list* **{10 | 100 | auto}**

| | |
|---|---|
| *port-list* | List of physical ports. MSS sets the port speed on all the specified ports. |
| **10** | Sets the port speed of a 10/100 Ethernet port to 10 Mbps and sets the operating mode to full-duplex. |
| **100** | Sets the port speed of a 10/100 Ethernet port to 100 Mbps and sets the operating mode to full-duplex. |
| **auto** | Enables a port to detect the speed and operating mode of the traffic on the link and set itself accordingly. |

**Defaults:** All ports are set to auto.

**Access:** Enabled.

**Usage:** D-Link recommends that you do not configure the mode of a switch port so that one side of the link is set to autonegotiation while the other side is set to full-duplex. Although MSS allows this configuration, it can result in slow throughput on the link. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex. A stream of large packets sent to a switch port in such a configuration can cause forwarding on the link to stop.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command sets the port speed on ports 1, 3 through 5, and 8 to 10 Mbps and sets the operating mode to full-duplex:

DWS-1008# **set port speed 1,3-5,8 10**

# set port trap

Enables or disables Simple Network Management Protocol (SNMP) linkup and linkdown traps on an individual port.

**Syntax: set port trap** *port-list* **{enable | disable}**

| | |
|---|---|
| *port-list* | List of physical ports. |
| **enable** | Enables the Telnet server. |
| **disable** | Disables the Telnet server. |

**Defaults:** SNMP linkup and linkdown traps are disabled by default.

**Access:** Enabled.

**Usage:** The **set port trap** command overrides the global setting of the **set snmp trap** command.

The **set port type** command does not affect the global trap information displayed by the **show snmp configuration** command. For example, if you globally enable linkup and linkdown traps but then disable the traps on a single port, the **show snmp configuration** command still indicates that the traps are globally enabled.

**Examples:** The following command enables SNMP linkup and linkdown traps on ports 5 and 6:

DWS-1008# **set port trap 5-6 enable**

**See Also:**
- set ip snmp server
- set snmp community
- set snmp trap
- set snmp trap receiver


Download from Www.Somanuals.com. All Manuals Search And Download.

# set port type ap

Configures a DWS-1008 switch port for an (AP) access point.

**Caution!** When you set the port type for AP use, you must specify the PoE state (enable or disable) of the port. Use the DWS-1008's PoE to power D-Link access points or PoE enabled devices only. If you enable PoE on a port connected to another device, physical damage to the device can result.

**Note:** Before configuring a port as an AP port, you must use the **set system countrycode** command to set the IEEE 802.11 country-specific regulations on the DWS-1008. See **set system countrycode**.

**Note:** For an AP that is indirectly connected to the DWS-1008 through an intermediate Layer 2 or Layer 3 network, use the **set dap** command to configure a Distributed AP.

**Note:** Before changing the port type from ap to wired-auth or from wired-auth to ap, you must reset the port with the **clear port type** command.

**Syntax: set port type ap** *port-list* **model {DWL-8200} poe {enable | disable} [radiotype {11a | 11b| 11g}]**

| | |
|---|---|
| *port-list* | List of physical ports. |
| **model** | Access: point model. |
| **poe enable \| disable** | Power over ethernet (PoE) state. |
| **radiotype 11a \| 11b \| 11g** | Radio type:<br>• **11a** - 802.11a<br>• **11b** - 802.11b<br>• **11g** - 802.11g<br><br>**Note:** This option applies only to single radio models. |

**Defaults:** All DWS-1008 ports are network ports by default.

**Access:** Enabled.

**Usage:** You cannot set a port's type if the port is a member of a port VLAN. To remove a port from a VLAN, use the **clear vlan** command. To reset a port as a network port, use the **clear port type** command.

When you change port type, MSS applies default settings appropriate for the port type. The following Table lists the default settings that MSS applies when you set a port's type to **ap**.


Download from Www.Somanuals.com. All Manuals Search And Download.

| Port Parameter | Setting |
|---|---|
| VLAN Membership | Removed from all VLANs. You cannot assign an AP access port to a VLAN. MSS automatically assigns AP access ports to VLANs based on user traffic. |
| Spanning Tree Protocol (STP) | Not applicable. |
| 802.1x | Uses authentication parameters configured for users. |
| Port Groups | Not applicable. |
| IGMP Snooping | Enabled as users are authenticated and join VLANs. |
| Maximum user sessions | Not applicable |

**Examples:** The following commands set port 2 for access point model DWL-8220AP, enables PoE on the port:

```
DWS-1008# set port type ap 2 model DWL-8220AP poe enable
This may affect the power applied on the configured ports. Would you like to continue?
(y/n) [n]y
success: change accepted.
```

**See Also:**
- clear dap
- clear port type
- set {ap | dap} radio antennatype
- set dap
- set port type wired-auth
- set system countrycode


Download from Www.Somanuals.com. All Manuals Search And Download.

# set port type wired-auth

Configures an DWS-1008 port for a wired authentication user.

**Syntax: set port type wired-auth** *port-list* **[tag** *tag-list***] [max-sessions** *num***] [auth-fall-thru {last-resort | none | web-portal}]**

| | |
|---|---|
| *port-list* | List of physical ports. |
| *tag-list* | One or more numbers between 1 and 4094 that subdivide a wired authentication port into virtual ports. |
| *num* | Maximum number of simultaneous user sessions supported. |
| **last-resort** | Automatically authenticates the user without requiring a user name and password. |
| **none** | Denies authentication and prohibits the user from accessing the network over this port. |
| **web-portal** | Serves the user a web page from the DWS-1008's nonvolatile storage for a secure login to the network. |

**Defaults:** The default tag-list is null (no tag values). The default number of sessions is 1. The default fallthru authentication type is none.

**Access:** Enabled.

**Usage:** You cannot set a port's type if the port is a member of a port VLAN. To remove a port from a VLAN, use the **clear vlan** command. To reset a port as a network port, use the **clear port type** command.

When you change port type, MSS applies default settings appropriate for the port type. The following Table lists the default settings that MSS applies when you set a port's type to **wired-auth**.

**Wired Authentication Port Defaults:**

| Port Parameter | Setting |
|---|---|
| VLAN Membership | Removed from all VLANs. You cannot assign an AP access port to a VLAN. MSS automatically assigns AP access ports to VLANs based on user traffic. |
| Spanning Tree Protocol (STP) | Not applicable. |
| 802.1x | Uses authentication parameters configured for users. |
| Port Groups | Not applicable. |
| IGMP Snooping | Enabled as users are authenticated and join VLANs. |
| Maximum user sessions | One (1) |
| Fallthru Auth type | None |


Download from Www.Somanuals.com. All Manuals Search And Download.

For 802.1X clients, wired authentication works only if the clients are directly attached to the wired authentication port, or are attached through a hub that does not block forwarding of packets from the client to the PAE group address (01:80:c2:00:00:03). Wired authentication works in accordance with the 802.1X specification, which prohibits a client from sending traffic directly to an authenticator's MAC address until the client is authenticated. Instead of sending traffic to the authenticator's MAC address, the client sends packets to the PAE group address. The 802.1X specification prohibits networking devices from forwarding PAE group address packets, because this would make it possible for multiple authenticators to acquire the same client.

For non-802.1X clients, who use MAC authentication, WebAAA, or last-resort authentication, wired authentication works if the clients are directly attached or indirectly attached.

**Examples:** The following command sets port 5 for a wired authentication user:

DWS-1008# **set port type wired-auth 5**
success: change accepted.

**Examples:** The following command sets port 6 for a wired authentication user and specifies a maximum of three simultaneous user sessions:

DWS-1008# **set port type wired-auth 6 max-sessions 3**
success: change accepted.

**See Also:**
- clear port type
- set port type


Download from Www.Somanuals.com. All Manuals Search And Download.

# show port counters

Displays port statistics.

**Syntax:** **show port counters [octets | packets | receive-errors | transmit-errors | collisions | receive-etherstats | transmit-etherstats] [port** *port-list***]**

| | |
|---|---|
| **octets** | Displays octet statistics. |
| **packets** | Displays packet statistics. |
| **receive-errors** | Displays errors in received packets. |
| **transmit-errors** | Displays errors in transmitted packets. |
| **collisions** | Displays collision statistics. |
| **receive-etherstats** | Displays Ethernet statistics for received packets. |
| **transmit-etherstats** | Displays Ethernet statistics for transmitted packets. |
| **port** *port-list* | List of physical ports. If you do not specify a port list, MSS displays statistics for all ports. |

**Defaults:** None.

**Access:** All.

**Usage:** You can specify one statistic type with the command.

**Examples:** The following command shows octet statistics for port 3:

```
DWS-1008> show port counters octets port 3
Port      Status      Rx Octets           Tx Octets
==========================================
3         Up          27965420            34886544
```

This command's output has the same fields as the **monitor port counters** command.

**See Also:**
- clear port counters
- monitor port counters


Download from Www.Somanuals.com. All Manuals Search And Download.

# show port-group

Displays port group information.

**Syntax: show port-group [name** *group-name***]**

**name** *group-name* Displays information for the specified port group.

**Defaults:** None.

**Access:** All.

**Examples:** The following command displays the configuration of port group server2:

```
DWS-1008# show port-group name server2
Port group: server2 is up
Ports: 3, 5
```

The table below describes the fields in the show port-group output.

| Field | Description |
|---|---|
| Port group | Name and state (enabled or disabled) of the port group. |
| Ports | Ports contained in the port group. |

**See Also:**
- clear port-group
- set port-group

# show port mirror

Displays the port mirroring configuration.

**Syntax: show port mirror**

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command displays the port mirroring configuration on the switch:

```
DWS-1008# show port mirror
Port 1 is mirrored to port 2
```

If port mirroring is not configured, the message in the following example is displayed instead:

```
DWS-1008# show port mirror
No ports are mirrored
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# show port poe

Displays status information for ports on which Power over Ethernet (PoE) is enabled.

**Syntax: show port poe [***port-list***]**

*port-list* List of physical ports. If you do not specify a port list, PoE information is displayed for all ports.

**Defaults:** None.

**Access:** All.

**Examples:** The following command displays PoE information for all ports on a DWS-1008:

```
DWS-1008# show port poe
                Link        Port        PoE         PoE
Port  Name Status      Type        config      Draw
=============================================================
1     1    up          -           disabled    off
2     2    down        -           disabled    off
3     3    down        -           disabled    off
4     4    down        -           disabled    off
5     5    down        -           disabled    off
6     6    up          AP          enabled     1.44
7     7    down        -           disabled    invalid
8     8    down        -           disabled    invalid
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Port | Port number. |
| Name | Port name. If the port does not have a name, the port number is listed. |
| Link status | Link status of the port:<br>• up—The port is connected.<br>• down—The port is not connected. |
| Port type | Port type:<br>• AP—The port is an AP access port.<br>• - (The port is not an AP access port.) |
| PoE config | PoE state:<br>• enabled<br>• disabled |
| PoE Draw | Power draw on the port, in watts.<br>For 10/100 Ethernet ports on which PoE is disabled, this field displays off. The value overcurrent indicates a PoE problem such as a short in the cable. |


Download from Www.Somanuals.com. All Manuals Search And Download.

# show port status

Displays configuration and status information for ports.

**Syntax: show port status [*port-list*]**

*port-list* List of physical ports. If you do not specify a port list, information is displayed for all ports.

**Defaults:** None.

**Access:** All.

**Examples:** The following command displays information for all ports on a DWS-1008:

```
DWS-1008# show port status
Port   Name    Admin   Oper   Config   Actual   Type      Media
=================================================================
1      1       up      up     auto     100/full network   10/100BaseTx
2      2       up      down   auto              network   10/100BaseTx
3      3       up      down   auto              network   10/100BaseTx
4      4       up      down   auto              network   10/100BaseTx
5      5       up      down   auto              network   10/100BaseTx
6      6       up      down   auto              network   10/100BaseTx
7      7       up      down   auto              network   no connector
8      8       up      down   auto              network   no connector
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Port | Port number. |
| Name | Port name. If the port does not have a name, the port number is listed. |
| Admin | Administrative status of the port:<br>• up—The port is enabled.<br>• down—The port is disabled. |
| Oper | Operational status of the port:<br>• up—The port is operational.<br>• down—The port is not operational. |
| Config | Port speed configured on the port:<br>• 10—10 Mbps.<br>• 100—100 Mbps.<br>• auto—The port sets its own speed. |
| Actual | Speed and operating mode in effect on the port. |
| Type | Port type:<br>• ap—AP access point port<br>• network—Network port<br>• wa—Wired authentication port |
| Media | Link type:<br>• 10/100BaseTX—10/100BASE-T. |


Download from Www.Somanuals.com. All Manuals Search And Download.

# VLAN Commands

Use virtual LAN (VLAN) commands to configure and manage parameters for individual port VLANs on network ports, and to display information about clients within a network. This chapter presents VLAN commands alphabetically. Use the following table to locate commands in this chapter based on their use.

| | |
|---|---|
| **Creation** | set vlan name on page 66 |
| **Ports** | set vlan port on page 67<br>clear vlan on page 62<br>show vlan config on page 71 |
| **Restriction of Client Layer 2 Forwarding** | set security l2-restrict on page 65<br>show security l2-restrict on page 70<br>clear security l2-restrict on page 61<br>clear security l2-restrict counters on page 62 |
| **FDB Entries** | set fdb on page 64<br>show fdb on page 68<br>show fdb count on page 70<br>clear fdb on page 60 |
| **FDB Aging Timeout** | set fdb agingtime on page 65<br>show fdb agingtime on page 69 |


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear fdb

Deletes an entry from the forwarding database (FDB).

**Syntax: clear fdb {perm | static | dynamic | port** *port-list***} [vlan** *vlan-id***] [tag** *tag-value***]**

| | |
|---|---|
| **perm** | Clears permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle. You must specify a VLAN name or number with this option. |
| **static** | Clears static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle. You must specify a VLAN name or number with this option. |
| **dynamic** | Clears dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle. You are not required to specify a VLAN name or number with this option. |
| **port** *port-lis* | Clears dynamic entries that match destination ports in the port list. You are not required to specify a VLAN name or number with this option. |
| **vlan** *vlan-id* | VLAN name or number—required for removing permanent and static entries. For dynamic entries, specifying a VLAN removes entries that match only that VLAN. Otherwise, dynamic entries that match all VLANs are removed. |
| **tag** *tag-value* | VLAN tag value that identifies a virtual port. If you do not specify a tag value, MSS deletes only entries that match untagged interfaces. Specifying a tag value deletes entries that match only the specified tagged interface. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** You can delete forwarding database entries based on entry type, port, or VLAN. A VLAN name or number is required for deleting permanent or static entries.

**Examples:** The following command clears all static forwarding database entries that match VLAN blue:

```
dws-1008# clear fdb static vlan blue
success: change accepted.
```

The following command clears all dynamic forwarding database entries that match all VLANs:

```
dws-1008# clear fdb dynamic
success: change accepted.
```

The following command clears all dynamic forwarding database entries that match ports 3 and 5:

```
dws-1008# clear fdb port 3,5
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear security l2-restrict

Removes one or more MAC addresses from the list of destination MAC addresses to which clients in a VLAN are allowed to send traffic at Layer 2.

**Syntax: clear security l2-restrict vlan** *vlan-id* **[permit-mac** *mac-addr* **[***mac-addr***] | all]**

| | |
|---|---|
| *vlan-id* | VLAN name or number. |
| **permit-mac** *mac-addr* [*mac-addr*] | List of MAC addresses. MSS no longer allows clients in the VLAN to send traffic to the MAC addresses at Layer 2. |
| **all** | Removes all MAC addresses from the list. |

**Defaults:** If you do not specify a list of MAC addresses or all, all addresses are removed.

**Access:** Enabled.

**Usage:** If you clear all MAC addresses, Layer 2 forwarding is no longer restricted in the VLAN. Clients within the VLAN will be able to communicate directly. There can be a slight delay before functions such as pinging between clients become available again after Layer 2 restrictions are lifted. Even though packets are passed immediately once Layer 2 restrictions are gone, it can take 10 seconds or more for upper-layer protocols to update their ARP caches and regain their functionality.

To clear the statistics counters without removing any MAC addresses, use the clear security l2-restrict counters command instead.

**Examples:** The following command removes MAC address aa:bb:cc:dd:ee:ff from the list of addresses to which clients in VLAN *abc_air* are allowed to send traffic at Layer 2:

```
DWS-1008# clear security l2-restrict vlan abc_air permit-mac aa:bb:cc:dd:ee:ff
success: change accepted.
```

**See Also:**
- clear security l2-restrict counters
- set security l2-restrict
- show security l2-restrict


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear security l2-restrict counters

Clear statistics counters for Layer 2 forwarding restriction.

**Syntax: clear security l2-restrict counters [vlan** *vlan-id* **| all]**

*vlan-id* VLAN name or number.

**all** Clears Layer 2 forwarding restriction counters for all VLANs.

**Defaults:** If you do not specify a VLAN or all, counters for all VLANs are cleared.

**Access:** Enabled.

**Usage:** To clear MAC addresses from the list of addresses to which clients are allowed to send data, use the **clear security l2-restrict** command instead.

**Examples:** The following command clears Layer 2 forwarding restriction statistics for VLAN *abc_air*:

```
DWS-1008# clear security l2-restrict counters vlan abc_air
success: change accepted.
```

**See Also:**
- clear security l2-restrict
- set security l2-restrict
- show security l2-restrict

# clear vlan

Removes physical or virtual ports from a VLAN or removes a VLAN entirely.

**Caution:** When you remove a VLAN, MSS completely removes the VLAN from the configuration and also removes all configuration information that uses the VLAN. If you want to remove only a specific port from the VLAN, make sure you specify the port number in the command.

**Syntax: clear vlan** *vlan-id* **[port** *port-list* **[tag** *tag-value***]]**

*vlan-id* VLAN name or number.

**port** *port-list* List of physical ports. MSS removes the specified ports from the VLAN. If you do not specify a list of ports, MSS removes the VLAN entirely.

**tag** *tag-value* Tag number that identifies a virtual port. MSS removes only the specified virtual port from the specified physical ports.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** Enabled.

**Usage:** If you do not specify a port-list, the entire VLAN is removed from the configuration.

**Note:** You cannot delete the default VLAN but you can remove ports from it. To remove ports from the default VLAN, use the **port** *port-list* option.

**Examples:** The following command removes port 1 from VLAN green:

```
DWS-1008# clear vlan green port 1
This may disrupt user connectivity. Do you wish to continue? (y/n) [n]y
success: change accepted.
```

The following command removes port 4, which uses tag value 69, from VLAN red:

```
DWS-1008# clear vlan red port 4 tag 69
This may disrupt user connectivity. Do you wish to continue? (y/n) [n]y
success: change accepted.
```

The following command completely removes VLAN marigold:

```
DWS-1008# clear vlan marigold
This may disrupt user connectivity. Do you wish to continue? (y/n) [n]y
success: change accepted.
```

**See Also:**
- set vlan port
- show vlan config


Download from Www.Somanuals.com. All Manuals Search And Download.

# set fdb

Adds a permanent or static entry to the forwarding database.

**Syntax: set fdb {perm | static}** *mac-addr* **port** *port-list* **vlan** *vlan-id* **[tag** *tag-value***]**

**perm** Adds a permanent entry. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.

**static** Adds a static entry. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.

*mac-addr* Destination MAC address of the entry. Use colons to separate the octets (for example, 00:11:22:aa:bb:cc).

**port** *port-list* List of physical destination ports for which to add the entry. A separate entry is added for each port you specify.

**vlan** *vlan-id* Name or number of a VLAN of which the port is a member. The entry is added only for the specified VLAN.

**tag** *tag-value* VLAN tag value that identifies a virtual port. You can specify a number from 1 through 4093. If you do not specify a tag value, an entry is created for an untagged interface only. If you specify a tag value, an entry is created only for the specified tagged interface.

**Defaults:** None.

**Access:** Enabled.

**Usage:** You cannot add a multicast or broadcast address as a permanent or static FDB entry.

**Examples:** The following command adds a permanent entry for MAC address 00:11:22:aa:bb:cc on ports 3 and 5 in VLAN *blue*:

```
DWS-1008# set fdb perm 00:11:22:aa:bb:cc port 3,5 vlan blue
success: change accepted.
```

The following command adds a static entry for MAC address 00:2b:3c:4d:5e:6f on port 1 in the default VLAN:

```
DWS-1008# set fdb static 00:2b:3c:4d:5e:6f port 1 vlan default
success: change accepted.
```

**See Also**
- clear fdb
- show fdb


Download from Www.Somanuals.com. All Manuals Search And Download.

# set fdb agingtime

Changes the aging timeout period for dynamic entries in the forwarding database.

**Syntax: set fdb agingtime** *vlan-id* **age** *seconds*

| | |
|---|---|
| *vlan-id* | VLAN name or number. The timeout period change applies only to entries that match the specified VLAN. |
| **age** *seconds* | Value for the timeout period, in seconds. You can specify a value from 0 through 1,000,000. If you change the timeout period to 0, aging is disabled. |

**Defaults:** The aging timeout period is 300 seconds (5 minutes).

**Access:** Enabled.

**Examples:** The following command changes the aging timeout period to 600 seconds for entries that match VLAN *orange*:

```
DWS-1008# set fdb agingtime orange age 600
success: change accepted.
```

**See Also:**
- show fdb agingtime

# set security l2-restrict

Restricts Layer 2 forwarding between clients in the same VLAN. When you restrict Layer 2 forwarding in a VLAN, MSS allows Layer 2 forwarding only between a client and a set of MAC addresses, generally the VLAN's default routers. Clients within the VLAN are not permitted to communicate among themselves directly. To communicate with another client, the client must use one of the specified default routers.

**Syntax: set security l2-restrict vlan** *vlan-id* **[mode {enable | disable}] [permit-mac** *mac-addr* **[***mac-addr***]]**

| | |
|---|---|
| *vlan-id* | VLAN name or number. |
| **mode {enable \| disable}** | Enables or disables restriction of Layer 2 forwarding. |
| **permit-mac** *mac-addr* **[***mac-addr***]** | MAC addresses to which clients are allowed to forward data at Layer 2. You can specify up to four addresses. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** Layer 2 restriction is disabled by default.

**Access:** Enabled.

**Usage:** You can specify multiple addresses by listing them on the same command line or by entering multiple commands. To change a MAC address, use the **clear security l2-restrict** command to remove it, then use the **set security l2-restrict** command to add the correct address.

Restriction of client traffic does not begin until you enable the permitted MAC list. Use the mode enable option with this command.

**Examples:** The following command restricts Layer 2 forwarding of client data in VLAN abc_air to the default routers with MAC address aa:bb:cc:dd:ee:ff and 11:22:33:44:55:66:

```
DWS-1008# set security l2-restrict vlan abc_air mode enable permit-mac
aa:bb:cc:dd:ee:ff 11:22:33:44:55:66
success: change accepted.
```

**See Also:**
- clear security l2-restrict
- clear security l2-restrict counters
- show security l2-restrict

# set vlan name

Creates a VLAN and assigns a number and name to it.

**Syntax: set vlan** *vlan-num* **name** *name*

| | |
|---|---|
| *vlan-num* | VLAN number. You can specify a number from 2 through 4093. |
| *name* | String up to 16 alphabetic characters long. |

**Defaults:** VLAN 1 is named default by default. No other VLANs have default names.

**Access:** Enabled.

**Usage:** You must assign a name to a VLAN (other than the default VLAN) before you can add ports to the VLAN.

D-Link recommends that you do not use the name default. This name is already used for VLAN 1. D-link also recommends that you do not rename the default VLAN. You cannot use a number as the first character in the VLAN name. D-Link recommends that you do not use the same name with different capitalizations for VLANs. For example, do not configure two separate VLANs with the names red and RED.


Download from Www.Somanuals.com. All Manuals Search And Download.

VLAN names are case-sensitive for RADIUS authorization when a client roams to a switch. If the switch is not configured with the VLAN the client is on, but is configured with a VLAN that has the same spelling but different capitalization, authorization for the client fails. For example, if the client is on VLAN red but the switch to which the client roams has VLAN RED instead, RADIUS authorization fails.

**Examples:** The following command assigns the name *marigold* to VLAN 3:

```
DWS-1008# set vlan 3 name marigold
success: change accepted.
```

**See Also:**
- set vlan port

# set vlan port

Assigns one or more network ports to a VLAN. You also can add a virtual port to each network port by adding a tag value to the network port.

**Syntax: set vlan** *vlan-id* **port** *port-list* **[tag** *tag-value***]**

| | |
|---|---|
| *vlan-id* | VLAN name or number. |
| **port** *port-list* | List of physical ports. |
| **tag** *tag-value* | Tag value that identifies a virtual port. You can specify a value from 1 through 4093. |

**Defaults:** By default, no ports are members of any VLANs. A switch cannot forward traffic on the network until you configure VLANs and add network ports to the VLANs.

**Access:** Enabled.

**Usage:** You can combine this command with the set port name command to assign the name and add the ports at the same time. If you do not specify a tag value, the switch sends untagged frames for the VLAN. If you do specify a tag value, the switch sends tagged frames only for the VLAN.

If you do specify a tag value, D-Link recommends that you use the same value as the VLAN number. MSS does not require the VLAN number and tag value to be the same but some other vendors' devices do.

**Examples:** The following command assigns the name beige to VLAN 11 and adds ports 1 through 3 to the VLAN:

```
DWS-1008# set vlan 11 name beige port 1-3
success: change accepted.
```

The following command adds port 5 to VLAN beige and assigns tag value 86 to the port:

```
DWS-1008# set vlan beige port 5 tag 86
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# show fdb

Displays entries in the forwarding database.

**Syntax:** **show fdb [***mac-addr-glob* **[vlan** *vlan-id***]]**
**show fdb {perm | static | dynamic | system | all} [port** *port-list* **|**
**vlan** *vlan-id***]**

| | |
|---|---|
| *mac-addr-glob* | A single MAC address or set of MAC addresses. Specify a MAC address, or use the wildcard character (*) to specify a set of MAC addresses. |
| **vlan** *vlan-id* | Name or number of a VLAN for which to display entries. |
| **perm** | Displays permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle. |
| **static** | Displays static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle. |
| **dynamic** | Displays dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle. |
| **system** | Displays system entries. A system entry is added by MSS. For example, the authentication protocols can add entries for wired and wireless authentication users. |
| **all** | Displays all entries in the database, or all the entries that match a particular port or ports or a particular VLAN. |

**port** *port-list* Destination port(s) for which to display entries.

**Defaults:** None.

**Access:** All.

**Usage:** To display the entire forwarding database, enter the **show fdb** command without options. To display only a portion of the database, use optional parameters to specify the types of entries you want to display.

**Examples:** The following command displays all entries in the forwarding database:

```
DWS-1008# show fdb all
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG    Dest MAC/Route Des      [CoS]        Destination Ports    [Protocol Type]
-------------------------------------------------------------------------------------------------------------
1           00:01:97:13:0b:1f                          1                [ALL]
1           aa:bb:cc:dd:ee:ff       *                  3                [ALL]
1           00:0b:0e:02:76:f5                          1                [ALL]
Total Matching FDB Entries Displayed = 3
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The top line of the display identifies the characters to distinguish among the entry types.

The following command displays all entries that begin with the MAC address glob 00:

```
DWS-1008# show fdb 00:*
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG    Dest MAC/Route Des      [CoS]      Destination Ports    [Protocol Type]
-----------------------------------------------------------------------------------------------------------
1           00:01:97:13:0b:1f                  1                    [ALL]
1           00:0b:0e:02:76:f5                  1                    [ALL]
Total Matching FDB Entries Displayed = 2
```

The table below describes the fields in the **show fdb** output.

| Field | Description |
|---|---|
| VLAN | VLAN number. |
| TAG | VLAN tag value. If the interface is untagged, the TAG field is blank. |
| Dest MAC/Route Des | MAC address of this forwarding entry's destination. |
| CoS | Type of entry. The entry types are explained in the first row of the ommand output.<br>**Note:** This Class of Service (CoS) value is not associated with MSS quality of service (QoS) features. |
| Destination Ports | Switch port associated with the entry. A switch sends traffic to the destination MAC address through this port. |
| Protocol Type | Layer 3 protocol address types that can be mapped to this entry. |
| Total Matching FDB Entries Displayed | Number of entries displayed by the command. |

# show fdb agingtime

Displays the aging timeout period for forwarding database entries.

**Syntax: show fdb agingtime [vlan** *vlan-id***]**

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, the aging timeout period for each VLAN is displayed.

**Defaults:** None.

**Access:** All.

**Examples:** The following command displays the aging timeout period for all VLANs:

```
DWS-1008# show fdb agingtime
VLAN 2 aging time = 600 sec
VLAN 1 aging time = 300 sec
```

Because the forwarding database aging timeout period can be configured only on an individual VLAN basis, the command lists the aging timeout period for each VLAN separately.


Download from Www.Somanuals.com. All Manuals Search And Download.

# show fdb count

Lists the number of entries in the forwarding database.

**Syntax: show fdb count {perm | static | dynamic} [vlan** *vlan-id***]**

**perm** Lists the number of permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.

**static** Lists the number of static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.

**dynamic** Lists the number of dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle.

**vlan** *vlan-id* VLAN name or number. Entries are listed for only the specified VLAN.

**Defaults:** None.

**Access:** All.

**Examples:** The following command lists the number of dynamic entries that the forwarding database contains:

```
DWS-1008# show fdb count dynamic
Total Matching Entries = 2
```

**See Also:**
- show fdb

# show security l2-restrict

Displays configuration information and statistics for Layer 2 forwarding restriction.

**Syntax: show security l2-restrict [vlan** *vlan-id* **| all]**

*vlan-id* VLAN name or number.

**all** Displays information for all VLANs.

**Defaults:** If you do not specify a VLAN name or all, information is displayed for all VLANs.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command shows Layer 2 forwarding restriction information for all VLANs:

```
DWS-1008# show security l2-restrict
VLAN  Name      En   Drops     Permit MAC          Hits
-----------------------------------------------------------------------------------------
1     default   Y    0         00:0b:0e:02:53:3e   5947
                                00:30:b6:3e:5c:a8   9
2     vlan-2    Y    0         04:04:04:04:04:04   0
```

The table describes the fields in the display.

| Field | Discription |
|---|---|
| VLAN | VLAN number. |
| Name | VLAN name. |
| En | Enabled state of the feature for the VLAN:<br>•Y—Enabled. Forwarding of Layer 2 traffic from clients is restricted to the MAC address(es) listed under Permit MAC.<br>• N—Disabled. Layer 2 forwarding is not restricted. |
| Drops | Number of packets dropped because the destination MAC address was not one of the addresses listed under Permit MAC. |
| Permit MAC | MAC addresses to which clients in the VLAN are allowed to send traffic at Layer 2. |
| Hits | Number of packets whose source MAC address was a client in this VLAN, and whose destination MAC address was one of those listed under Permit MAC. |

**See Also:**
- clear security l2-restrict
- clear security l2-restrict counters
- set security l2-restrict

# show vlan config

Displays VLAN information.

**Syntax: show vlan config [*vlan-id*]**

*vlan-id* VLAN name or number. If you do not specify a VLAN, information for all VLANs is displayed.

**Defaults:** None.

**Access:** All.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command displays information for VLAN burgundy:

```
DWS-1008# show vlan config burgundy
                        Admin       VLAN        Tunl                    Port
VLAN  Name              Status      State       Affin   Port    Tag     State
-------------------------------------------------------------------------------
2     burgundy          Up          Up          5
                                                      2       none    Up
                                                      3       none    Up
                                                      4       none    Up
                                                      5       none    Up
                                                      6       none    Up
                                                t:10.10.40.4  none    Up
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| VLAN | VLAN number. |
| Name | VLAN name. |
| Admin Status | Administrative status of the VLAN:<br>• Down—The VLAN is disabled.<br>• Up—The VLAN is enabled. |
| VLAN State | Link status of the VLAN:<br>• Down—The VLAN is not connected.<br>• Up—The VLAN is connected. |
| Tunl Affin | Tunnel affinity value assigned to the VLAN. |
| Port | Member port of the VLAN. The port can be a physical port or a virtual port.<br>• Physical ports are 10/100 Ethernet on the switch, and are listed by port number.<br>• Virtual ports are tunnels to other switches in a mobility domain, and are listed as follows: t:ip-addr, where ip-addr is the system IP address of the switch at the other end of the tunnel.<br>**Note:** This field can include AP access ports and wired authentication ports, because MSS dynamically adds these ports to a VLAN when handling user traffic for the VLAN. |
| Tag | Tag value assigned to the port. |
| Port State | Link state of the port:<br>• Down—The port is not connected.<br>• Up—The port is connected. |

**See Also:**
- clear vlan
- set vlan name
- set vlan port


Download from Www.Somanuals.com. All Manuals Search And Download.

# Quality of Service Commands

Use Quality of Service (QoS) commands to configure packet prioritization in MSS. Packet prioritization ensures that DWS-1008 switches and DWL-8220AP access points give preferential treatment to high-priority traffic such as voice and video.

This chapter presents QoS commands alphabetically. Use the following table to locate commands in this chapter based on their use.


| | |
|---|---|
| **QoS Settings** | show qos on page 75 |
| | show qos dscp-table on page 76 |
| | set qos cos-to-dscp-map on page 74 |
| | set qos dscp-to-cos-map on page 75 |
| | clear qos on page 74 |


## clear qos

Resets the switch's mapping of Differentiated Services Code Point (DSCP) values to internal QoS values.

The switch's internal QoS map ensures that prioritized traffic remains prioritized while transiting through the DWS-1008 switch. A switch uses the QoS map to do the following:

- Classify inbound packets by mapping their DSCP values to one of eight internal QoS values
- Classify outbound packets by marking their DSCP values based on the switch's internal QoS values

**Syntax: clear qos [cos-to-dscp-map [*from-qos*] | dscp-to-cos-map [*from-dscp*]]**

| | |
|---|---|
| **cos-to-dscp-map** [*from-qos*] | Resets the mapping between the specified internal QoS value and the DSCP values with which MSS marks outbound packets. QoS values are from 0 to 7. |
| **dscp-to-cos-map** [*from-dscp*] | Resets the mapping between the specified range of DSCP values and internal QoS value with which MSS classifies inbound packets. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** Enabled.

**Usage:** To reset all mappings to their default values, use the clear qos command without the optional parameters.

**Examples:** The following command resets all QoS mappings:

```
DWS-1008# clear qos
success: change accepted.
```

The following command resets the mapping used to classify packets with DSCP value 44:

```
DWS-1008# clear qos dscp-to-qos-map 44
success: change accepted.
```

## set qos cos-to-dscp-map

Changes the value to which MSS maps an internal QoS value when marking outbound packets.

**Syntax**: **set qos cos-to-dscp-map** *level* **dscp** *dscp-value*

| | |
|---|---|
| **level** | Internal CoS value. You can specify a number from 0 to 7. |
| **dscp** *dscp-value* | DSCP value. You can specify the value as a decimal number. Valid values are 0 to 63. |

**Defaults:** The defaults are listed by the **show qos** command.

**Access:** Enabled.

**Examples:** The following command maps internal CoS value 5 to DSCP value 50:

```
DWS-1008# set qos cos-to-dscp-map 5 dscp 50
warning: cos 5 is marked with dscp 50 which will be classified as cos 6
```

If the change results in a change to CoS, MSS displays a warning message indicating the change. In this example, packets that receive CoS 5 upon ingress will be marked with a DSCP value equivalent to CoS 6 upon egress.

**See Also:**
- set qos dscp-to-cos-map
- show qos


Download from Www.Somanuals.com. All Manuals Search And Download.

# set qos dscp-to-cos-map

Changes the internal QoS value to which MSS maps a packet's DSCP value when classifying inbound packets.

**Syntax: set qos dscp-to-cos-map** *dscp-range* **cos** *level*

*dscp-range* DSCP range. You can specify the values as decimal numbers. Valid decimal values are 0 to 63. To specify a range, use the following format: 40-56. Specify the lower number first.

**cos** *level* Internal QoS value. You can specify a number from 0 to 7.

**Defaults:** The defaults are listed by the **show qos** command.

**Access:** Enabled.

**Examples:** The following command maps DSCP values 40-56 to internal CoS value 6:

```
DWS-1008# set qos dscp-to-cos-map 40-56 cos 6
warning: cos 5 is marked with dscp 63 which will be classified as cos 7
warning: cos 7 is marked with dscp 56 which will be classified as cos 6
```

As shown in this example, if the change results in a change to CoS, MSS displays a warning message indicating the change.

**See Also:**
- set qos cos-to-dscp-map
- show qos

# show qos

Displays the switch's QoS settings.

**Syntax: show qos [default]**

**default** Displays the default mappings.

**Defaults:** None.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command displays the default QoS settings:

DWS-1008# **show qos default**

Ingress QoS Classification Map (dscp-to-cos)

| Ingress DSCP | CoS Level | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 00-09 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 10-19 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 |
| 20-29 | 2 | 2 | 2 | 2 | 3 | 3 | 3 | 3 | 3 | 3 |
| 30-39 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 40-49 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 6 | 6 |
| 50-59 | 6 | 6 | 6 | 6 | 6 | 6 | 7 | 7 | 7 | 7 |
| 60-63 | 7 | 7 | 7 | 7 | | | | | | |

Egress QoS Marking Map (cos-to-dscp)

| CoS Level | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Egress DSCP | 0 | 8 | 16 | 24 | 32 | 40 | 48 | 56 |
| Egress ToS byte | 0x00 | 0x20 | 0x40 | 0x60 | 0x80 | 0xA0 | 0xC0 | 0xE0 |

**See Also:**
• show qos dscp-table

# show qos dscp-table

Displays a table that maps Differentiated Services Code Point (DSCP) values to their equivalent combinations of IP precedence values and IP ToS values.

**Syntax: show qos dscp-table**

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command displays the table:

DWS-1008# **show qos dscp-table**

| DSCP | | TOS | | precedence | tos |
|---|---|---|---|---|---|
| dec | hex | dec | hex | | |
| 0 | 0x00 | 0 | 0x00 | 0 | 0 |
| 1 | 0x01 | 4 | 0x04 | 0 | 2 |
| 2 | 0x02 | 8 | 0x08 | 0 | 4 |
| ... | | | | | |
| 63 | 0x3f | 252 | 0xfc | 7 | 14 |

**See Also:**
• show qos


Download from Www.Somanuals.com. All Manuals Search And Download.

# IP Services Commands

Use IP services commands to configure and manage IP interfaces, management services, the Domain Name Service (DNS), Network Time Protocol (NTP), and aliases, and to ping a host or trace a route. This chapter presents IP services commands alphabetically.

## clear interface

Removes an IP interface.

**Syntax: clear interface** *vlan-id* **ip**

*vlan-id* VLAN name or number.

**Defaults:** None.

**Access:** Enabled.

**Usage:** If the interface you want to remove is configured as the system IP address, removing the address can interfere with system tasks that use the system IP address, including the following:

- Topology reporting for dual-homed access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

**Examples:** The following command removes the IP interface configured on VLAN mauve:

```
DWS-1008# clear interface mauve ip
success: cleared ip on vlan mauve
```

**See Also:**
- set interface
- set interface status
- show interface


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear ip alias

Removes an alias, which is a string that represents an IP address.

**Syntax: clear ip alias** *name*

*name* Alias name.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes the alias *server1*:

```
DWS-1008# clear ip alias server1
success: change accepted.
```

**See Also:**
- set ip alias
- show ip alias

# clear ip dns domain

Removes the default DNS domain name.

**Syntax: clear ip dns domain**

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes the default DNS domain name from a switch:

```
DWS-1008# clear ip dns domain
Default DNS domain name cleared.
```

**See Also:**
- clear ip dns server
- set ip dns
- set ip dns domain
- set ip dns server
- show ip dns


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear ip dns server

Removes a DNS server from a DWS-1008 switch configuration.

**Syntax: clear ip dns server** *ip-addr*

*ip-addr* IP address of a DNS server.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes DNS server 10.10.10.69 from a switch's configuration:

```
DWS-1008# clear ip dns server 10.10.10.69
success: change accepted.
```

**See Also:**
- clear ip dns domain
- set ip dns
- set ip dns domain
- set ip dns server
- show ip dns

# clear ip route

Removes a route from the IP route table.

**Syntax: clear ip route {default |** *ip-addr mask* **|** *ip-addr/mask-length***}** *default-router*

**default** Default route. Note: default is an alias for IP address 0.0.0.0/0.

*ip-addr mask* IP address and subnet mask for the route destination, in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).

*ip-addr/mask-length* IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).

*default-router* IP address, DNS hostname, or alias of the next-hop router.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes the route to destination 10.10.10.68/24 through router 10.10.10.1:

```
DWS-1008# clear ip route 10.10.10.68/24 10.10.10.1
success: change accepted.
```

**See Also:**
- set ip route
- show ip route

# clear ip telnet

Resets the Telnet server's TCP port number to its default value. A DWS-1008 switch listens for Telnet management traffic on the Telnet server port.

**Syntax: clear ip telnet**

**Defaults:** The default Telnet port number is 23.

**Access:** Enabled.

**Examples:** The following command resets the TCP port number for Telnet management traffic to its default:

```
DWS-1008# clear ip telnet
success: change accepted.
```

**See Also:**
- set ip https server
- set ip telnet
- set ip telnet server
- show ip https
- show ip telnet


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear ntp server

Removes an NTP server from a switch configuration.

**Syntax: clear ntp server {***ip-addr* **| all}**

*ip-addr* IP address of the server to remove, in dotted decimal notation.

**all** Removes all NTP servers from the configuration.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes NTP server 192.168.40.240 from a switch configuration:

```
DWS-1008# clear ntp server 192.168.40.240
success: change accepted.
```

**See Also:**
- clear ntp update-interval
- set ntp
- set ntp server
- set ntp update-interval
- show ntp

# clear ntp update-interval

Resets the NTP update interval to the default value.

**Syntax: clear ntp update-interval**

**Defaults:** The default NTP update interval is 64 seconds.

**Access:** Enabled.

**Examples:** To reset the NTP interval to the default value, type the following command:

```
DWS-1008# clear ntp update-interval
success: change accepted.
```

**See Also:**
- clear ntp server
- set ntp
- set ntp server
- set ntp update-interval
- show ntp


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear snmp community

Clears an SNMP community string.

**Syntax: clear snmp community name** *comm-string*

*comm-string* Name of the SNMP community you want to clear.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command clears community string setswitch2:

```
DWS-1008# clear snmp community name setswitch2
success: change accepted.
```

**See Also:**
- set snmp community
- show snmp community

# clear snmp notify profile

Clears an SNMP notification profile.

**Syntax: clear snmp notify profile** *profile-name*

*profile-name* Name of the notification profile you are clearing.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command clears notification profile *snmpprof_rfdetect*:

```
DWS-1008# clear snmp notify profile snmpprof_rfdetect
success: change accepted.
```

**See Also:**
- set snmp notify profile
- show snmp notify profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear snmp notify target

Clears an SNMP notification target.

**Syntax: clear snmp notify target** *target-num*

*target-num* ID of the target.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command clears notification target 3:

```
DWS-1008# clear snmp notify target 3
success: change accepted.
```

**See Also:**
- set snmp notify target
- show snmp notify target

# clear snmp usm

Clears an SNMPv3 user.

**Syntax: clear snmp usm** *usm-username*

*usm-username* Name of the SNMPv3 user you want to clear.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command clears SNMPv3 user *snmpmgr1*:

```
DWS-1008# clear snmp usm snmpmgr1
success: change accepted.
```

**See Also:**
- set snmp usm
- show snmp usm


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear summertime

Clears the summertime setting from a DWS-1008 switch.

**Syntax: clear summertime**

**Defaults:** None.

**Access:** Enabled.

**Examples:** To clear the summertime setting from a switch, type the following command:

```
DWS-1008# clear summertime
success: change accepted.
```

**See Also:**
- clear timezone
- set summertime
- set timedate
- set timezone
- show summertime
- show timedate
- show timezone

# clear system ip-address

Clears the system IP address.

**Caution:** Clearing the system IP address disrupts the system tasks that use the address.

**Syntax: clear system ip-address**

**Defaults:** None.

**Access:** Enabled.

**Usage:** Clearing the system IP address can interfere with system tasks that use the system IP address, including the following:

- Topology reporting for dual-homed access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

**Examples:** To clear the system IP address, type the following command:

```
DWS-1008# clear system ip-address
success: change accepted.
```

**See Also:**
- set system ip-address
- show system


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear timezone

Clears the time offset for the switch's real-time clock from Coordinated Universal Time (UTC). UTC is also know as Greenwich Mean Time (GMT).

**Syntax:** clear timezone

**Defaults:** None.

**Access:** Enabled.

**Examples:** To return the switch's real-time clock to UTC, type the following command:

```
DWS-1008# clear timezone
success: change accepted.
```

**See Also:**
- clear summertime
- set summertime
- set timedate
- set timezone
- show summertime
- show timedate
- show timezone

# ping

Tests IP connectivity between a switch and another device. MSS sends an Internet Control Message Protocol (ICMP) echo packet to the specified device and listens for a reply packet.

**Syntax: ping** *host* **[count** *num-packets***] [dnf] [flood] [interval** *time***] [size** *size***]**
**[source-ip** *ip-addr* **|** *vlan-name***]**

| | |
|---|---|
| *host* | IP address, MAC address, hostname, alias, or user to ping. |
| **count** *num-packets* | Number of ping packets to send. You can specify from 0 through 2,147,483,647. If you enter 0, MSS pings continuously until you interrupt the command. |
| **dnf** | Enables the Do Not Fragment bit in the ping packet to prevent the packet from being fragmented. |
| **flood** | Sends new ping packets as quickly as replies are received, or 100 times per second, whichever is greater.<br><br>**Note:** Use the flood option sparingly. This option creates a lot of traffic and can affect other traffic on the network. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| *interval time* | Time interval between ping packets, in milliseconds. You can specify from 100 through 10,000. |
| **size** *size* | Packet size, in bytes. You can specify from 56 through 65,507.<br>**Note:** Because the switch adds header information, the ICMP packet size is 8 bytes larger than the size you specify. |
| **source-ip** *ip-addr* | IP address, in dotted decimal notation, to use as the source IP address in the ping packets. |
| **source-ip** *vlan-name* | VLAN name to use as the ping source. MSS uses the IP address configured on the VLAN as the source IP address in the ping packets. |

**Defaults:**
- count—5.
- dnf—Disabled.
- interval—100 (one tenth of a second)
- size—56.

**Access:** Enabled.

**Usage:** To stop a ping command that is in progress, press Ctrl+C. A DWS-1008 switch cannot ping itself. MSS does not support this.

**Examples:** The following command pings a device that has IP address 10.1.1.1:

```
DWS-1008# ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1) from 10.9.4.34 : 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.769 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.628 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.676 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.619 ms
64 bytes from 10.1.1.1: icmp_seq=5 ttl=255 time=0.608 ms
--- 10.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0 errors, 0% packet loss
```

**See Also:**
- traceroute


Download from Www.Somanuals.com. All Manuals Search And Download.

# set arp

Adds an ARP entry to the ARP table.

**Syntax: set arp {permanent | static | dynamic}** *ip-addr mac-addr*

| | |
|---|---|
| **permanent** | Adds a permanent entry. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle. |
| **static** | Adds a static entry. A static entry does not age out, but the entry does not remain in the database after a reboot, reset, or power cycle. |
| **dynamic** | Adds a dynamic entry. A dynamic entry is automatically removed if the entry ages out, or after a reboot, reset, or power cycle. |
| *ip-addr* | IP address of the entry, in dotted decimal notation. |
| *mac-addr* | MAC address to map to the IP address. Use colons to separate the octets (for example, 00:11:22:aa:bb:cc). |

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command adds a static ARP entry that maps IP address 10.10.10.1 to MAC address 00:bb:cc:dd:ee:ff:

```
DWS-1008# set arp static 10.10.10.1 00:bb:cc:dd:ee:ff
success: added arp 10.10.10.1 at 00:bb:cc:dd:ee:ff on VLAN 1
```

**See Also:**
- set arp agingtime
- show arp

# set arp agingtime

Changes the aging timeout for dynamic ARP entries.

**Syntax: set arp agingtime** *seconds*

| | |
|---|---|
| *seconds* | Number of seconds an entry can remain unused before MSS removes the entry. You can specify from 0 through 1,000,000. To disable aging, specify 0. |

**Defaults:** The default aging timeout is 1200 seconds.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Access:** Enabled.

**Usage:** Aging applies only to dynamic entries.

To reset the ARP aging timeout to its default value, use the set arp agingtime 1200 command.

**Examples:** The following command changes the ARP aging timeout to 1800 seconds:

```
DWS-1008# set arp agingtime 1800
success: set arp aging time to 1800 seconds
```

The following command disables ARP aging:

```
DWS-1008# set arp agingtime 0
success: set arp aging time to 0 seconds
```

**See Also:**
- set arp
- show arp

# Set interface

Configures an IP interface on a VLAN.

**Syntax: set interface** *vlan-id* **ip {***ip-addr mask* **|** *ip-addr/mask-length***}**

| | |
|---|---|
| *vlan-id* | VLAN name or number. |
| *ip-addr mask* | IP address and subnet mask in dotted decimal notation (for example, 10.10.10.10 255.255.255.0). |
| *ip-addr/mask-length* | IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24). |

**Defaults:** None.

**Access:** Enabled.

**Usage:** You can assign one IP interface to each VLAN.

If an interface is already configured on the VLAN you specify, this command replaces the interface. If you replace an interface that is in use as the system IP address, replacing the interface can interfere with system tasks that use the system IP address, including the following:

- Topology reporting for dual-homed access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command configures IP interface 10.10.10.10/24 on VLAN *default*:

```
DWS-1008# set interface default ip 10.10.10.10/24
success: set ip address 10.10.10.10 netmask 255.255.255.0 on vlan default
```

The following command configures IP interface 10.10.20.10 255.255.255.0 on VLAN *mauve*:

```
DWS-1008# set interface mauve ip 10.10.20.10 255.255.255.0
success: set ip address 10.10.20.10 netmask 255.255.255.0 on vlan mauve
```

**See Also:**
- clear interface
- set interface status
- show interface

# set interface dhcp-client

Configures the DHCP client on a VLAN, to allow the VLAN to obtain its IP interface from a DHCP server.

**Syntax: set interface** *vlan-id* **ip dhcp-client {enable | disable}**

*vlan-id* VLAN name or number.

**enable** Enables the DHCP client on the VLAN.

**disable** Disables the DHCP client on the VLAN.

**Defaults:** The DHCP client is disabled by default on the DWS-1008.

**Access:** Enabled.

**Usage:** You can enable the DHCP client on one VLAN only. You can configure the DHCP client on more than one VLAN, but the client can be active on only one VLAN.

MSS also has a configurable DHCP server. You can configure a DHCP client and DHCP server on the same VLAN, but only the client or the server can be enabled. The DHCP client and DHCP server cannot both be enabled on the same VLAN at the same time.

**Examples:** The following command enables the DHCP client on VLAN corpvlan:

```
DWS-1008# set interface corpvlan ip dhcp-client enable
success: change accepted.
```

**See Also:**
- clear interface
- show dhcp-client
- show interface


Download from Www.Somanuals.com. All Manuals Search And Download.

# set interface dhcp-server

Configures the MSS DHCP server.

**Note:** Use of the MSS DHCP server to allocate client addresses is intended for temporary, demonstration deployments and not for production networks. D-Link recommends that you do not use the MSS DHCP server to allocate client addresses in a production network.

**Syntax: set interface** *vlan-id* **ip dhcp-server [enable | disable] [start** *ip-addr1* **stop** *ip-addr2***] [dns-domain** *domain-name***] [primary-dns** *ip-addr* **[secondary-dns** *ip-addr***]] [default-router** *ip-addr***]**

| | |
|---|---|
| *vlan-id* | VLAN name or number. |
| **enable** | Enables the DHCP server. |
| **disable** | Disables the DHCP server. |
| **start** *ip-addr1* | Specifies the beginning address of the address range (also called the address pool). |
| **stop** *ip-addr2* | Specifies the ending address of the address range. |
| **dns-domain** *domain-name* | Name of the DHCP client's default DNS domain. |
| **primary-dns** *ip-addr* **[secondary-dns** *ip-addr***]** | IP addresses of the DHCP client's DNS servers. |
| **default-router** *ip-addr* | IP address of the DHCP client's default router. |

**Defaults:** The DHCP server is enabled by default on a new (unconfigured) DWS-1008 in order to provide an IP address to the host connected to the switch for access to the Web Quick Start.

**Access:** Enabled.

**Usage:** By default, all addresses except the host address of the VLAN, the network broadcast address, and the subnet broadcast address are included in the range. If you specify the range, the start address must be lower than the stop address, and all addresses must be in the same subnet. The IP interface of the VLAN must be within the same subnet but is not required to be within the range.

Specification of the DNS domain name, DNS servers, and default router are optional. If you omit one or more of these options, the MSS DHCP server uses oath values configured elsewhere on the switch:

- DNS domain name—If this option is not set with the **set interface dhcp-server** command's dns-domain option, the MSS DHCP server uses the value set by the set ip dns domain command.


Download from Www.Somanuals.com. All Manuals Search And Download.

- DNS servers—If these options are not set with the set interface dhcp-server command's primary-dns and secondary-dns options, the MSS DHCP server uses the values set by the set ip dns server command.

- Default router—If this option is not set with the set interface dhcp-server command's default-router option, the MSS DHCP server can use the value set by the set ip route command. A default route configured by set ip route can be used if the route is in the DHCP client's subnet. Otherwise, the MSS DHCP server does not specify a router address.

**Examples:** The following command enables the DHCP server on VLAN *red-vlan* to serve addresses from the 192.168.1.5 to 192.168.1.25 range:

```
DWS-1008# set interface red-vlan ip dhcp-server enable start 192.168.1.5 stop
      192.168.1.25
success: change accepted.
```

**See Also:**
- set ip dns domain
- set ip dns server
- show dhcp-server

# set interface status

Administratively disables or reenables an IP interface.

**Syntax: set interface** *vlan-id* **status {up | down}**

*vlan-id* VLAN name or number.

**up** Enables the interface.

**down** Disables the interface.

**Defaults:** IP interfaces are enabled by default.

**Access:** Enabled.

**Examples:** The following command disables the IP interface on VLAN mauve:

```
DWS-1008# set interface mauve status down
success: set interface mauve to down
```

**See Also:**
- clear interface
- set interface
- show interface


Download from Www.Somanuals.com. All Manuals Search And Download.

# set ip alias

Configures an alias, which maps a name to an IP address. You can use aliases as shortcuts in CLI commands.

**Syntax: set ip alias** *name ip-addr*

*name* String of up to 32 alphanumeric characters, with no spaces.

*ip-addr* IP address in dotted decimal notation.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command configures the alias *HR1* for IP address 192.168.1.2:

```
DWS-1008# set ip alias HR1 192.168.1.2
success: change accepted.
```

**See Also:**
- clear ip alias
- show ip alias

# set ip dns

Enables or disables DNS on a DWS-1008 switch.

**Syntax: set ip dns {enable | disable}**

**enable** Enables DNS.

**disable** Disables DNS.

**Defaults:** DNS is disabled by default.

**Access:** Enabled.

**Examples:** The following command enables DNS on a DWS-1008 switch:

```
DWS-1008# set ip dns enable
Start DNS Client
```

**See Also:**
- clear ip dns domain
- clear ip dns server
- set ip dns domain
- set ip dns server
- show ip dns


Download from Www.Somanuals.com. All Manuals Search And Download.

# set ip dns domain

Configures a default domain name for DNS queries. The switch appends the default domain name to domain names or hostnames you enter in commands.

**Syntax: set ip dns domain** *name*

*name* Domain name of between 1 and 64 alphanumeric characters with no spaces (for example, example.org).

**Defaults:** None.

**Access:** Enabled.

**Usage:** To override the default domain name when entering a hostname in a CLI command, enter a period at the end of the hostname. For example, if the default domain name is example.com, enter chris. if the fully qualified hostname is chris and not chris.example.com.

Aliases take precedence over DNS. When you enter a hostname, MSS checks for an alias with that name first, before using DNS to resolve the name.

**Examples:** The following command configures the default domain name example.com:

```
DWS-1008# set ip dns domain example.com
Domain name changed
```

**See Also:**
- clear ip dns domain
- clear ip dns server
- set ip dns

# set ip dns server

Specifies a DNS server to use for resolving hostnames you enter in CLI commands.

**Syntax: set ip dns server** *ip-addr* **{primary | secondary}**

*ip-addr* IP address of a DNS server, in dotted decimal or CIDR notation.

**primary** Makes the server the primary server, which MSS always consults first for resolving DNS queries.

**secondary** Makes the server a secondary server. MSS consults a secondary server only if the primary server does not reply.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** Enabled.

**Usage:** You can configure a DWS-1008 switch to use one primary DNS server and up to five secondary DNS servers.

**Examples:** The following commands configure a DWS-1008 switch to use a primary DNS server and two secondary DNS servers:

```
DWS-1008# set ip dns server 10.10.10.50/24 primary
success: change accepted.
DWS-1008# set ip dns server 10.10.20.69/24 secondary
success: change accepted.
DWS-1008# set ip dns server 10.10.30.69/24 secondary
success: change accepted.
```

**See Also:**
- clear ip dns domain
- clear ip dns server
- set ip dns
- set ip dns domain
- show ip dns

# set ip https server

Enables the HTTPS server on a DWS-1008 switch. The HTTPS server is required for Web View access to the switch.

**Caution:** If you disable the HTTPS server, Web View access to the switch is disabled.

**Syntax: set ip https server {enable | disable}**

**enable** Enables the HTTPS server.

**disable** Disables the HTTPS server.

**Defaults:** The HTTPS server is disabled by default.

**Access:** Enabled.

**Examples:** The following command enables the HTTPS server on a DWS-1008 switch:

```
DWS-1008# set ip https server enable
success: change accepted.
```

**See Also:**
- clear ip telnet
- set ip telnet
- set ip telnet server
- show ip https
- show ip telnet


Download from Www.Somanuals.com. All Manuals Search And Download.

# set ip route

Adds a static route to the IP route table.

**Syntax: set ip route {default |** *ip-addr mask* **|** *ip-addr/mask-length***}** *default-router metric*

| | |
|---|---|
| **default** | Default route. A DWS-1008 switch uses the default route if an explicit route is not available for the destination.<br><br>**Note:** default is an alias for IP address 0.0.0.0/0. |
| *ip-addr mask* | IP address and subnet mask for the route destination, in dotted decimal notation (for example, 10.10.10.10 255.255.255.0). |
| *ip-addr/mask-length* | IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24). |
| *default-router* | IP address, DNS hostname, or alias of the next-hop router. |
| *metric* | Cost for using the route. You can specify a value from 0 through 2,147,483,647. Lower-cost routes are preferred over higher-cost routes. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** MSS can use a static route only if a direct route in the route table resolves the static route. MSS adds routes with next-hop types Local and Direct when you add an IP interface to a VLAN, if the VLAN is up. If one of these added routes can resolve the static route, MSS can use the static route.

Before you add a static route, use the show interface command to verify that the switch has an IP interface in the same subnet as the route's next-hop router. If not, the VLAN:Interface field of the **show ip route** command output shows that the route is down.

You can configure a maximum of 4 routes per destination. This includes default routes, which have destination 0.0.0.0/0. Each route to a given destination must have a unique router address. When the route table contains multiple default or explicit routes to the same destination, MSS uses the route with the lowest cost. If two or more routes to the same destination have the lowest cost, MSS selects the first route in the route table.

When you add multiple routes to the same destination, MSS groups the routes and orders them from lowest cost at the top of the group to highest cost at the bottom of the group. If you add a new route that has the same destination and cost as a route already in the table, MSS places the new route at the top of the group of routes with the same cost.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command adds a default route that uses default router 10.5.4.1 and gives the route a cost of 1:

```
DWS-1008# set ip route default 10.5.4.1 1
success: change accepted.
```

The following commands add two default routes, and configure MSS to always use the route through 10.2.4.69 when the switch interface to that default router is up:

```
DWS-1008# set ip route default 10.2.4.69 1
success: change accepted.

DWS-1008# set ip route default 10.2.4.17 2
success: change accepted.
```

The following command adds an explicit route from a DWS-1008 switch to any host on the 192.168.4.x subnet through the local router 10.5.4.2, and gives the route a cost of 1:

```
DWS-1008# set ip route 192.168.4.0 255.255.255.0 10.5.4.2 1
success: change accepted.
```

The following command adds another explicit route, using CIDR notation to specify the subnet mask:

```
DWS-1008# set ip route 192.168.5.0/24 10.5.5.2 1
success: change accepted.
```

**See Also:**
- clear ip route
- show interface
- show ip route

# set ip snmp server

Enables or disables the SNMP service on the DWS-1008 switch.

**Syntax: set ip snmp server {enable | disable}**

**enable** Enables the SNMP service.

**disable** Disables the SNMP service.

**Defaults:** The SNMP service is disabled by default.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command enables the SNMP server on a DWS-1008 switch:

```
DWS-1008# set ip snmp server enable
success: change accepted.
```

**See Also:**
- clear snmp trap receiver
- set port trap
- set snmp community
- set snmp trap
- set snmp trap receiver
- show snmp configuration

# set ip ssh

Changes the TCP port number on which a DWS-1008 switch listens for Secure Shell (SSH) management traffic.

**Caution:** If you change the SSH port number from an SSH session, MSS immediately ends the session. To open a new management session, you must configure the SSH client to use the new TCP port number.

**Syntax: set ip ssh port** *port-num*

*port-num* TCP port number.

**Defaults:** The default SSH port number is 22.

**Access:** Enabled.

**Examples:** The following command changes the SSH port number on a DWS-1008 switch to 6000:

```
DWS-1008# set ip ssh port 6000
success: change accepted.
```

**See Also:**
- set ip ssh server


Download from Www.Somanuals.com. All Manuals Search And Download.

# set ip ssh server

Disables or reenables the SSH server on a switch.

**Caution:** If you disable the SSH server, SSH access to the switch is also disabled.

**Syntax: set ip ssh server {enable | disable}**

**enable** Enables the SSH server.

**disable** Disables the SSH server.

**Defaults:** The SSH server is enabled by default.

**Access:** Enabled.

**Usage:** SSH requires an SSH authentication key. You can generate one or allow MSS to generate one. The first time an SSH client attempts to access the SSH server on a DWS-1008 switch, the switch automatically generates a 1024-byte SSH key.

If you want to use a 2048-byte key instead, use the **crypto generate key ssh 2048** command to generate one.

The maximum number of SSH sessions supported on a DWS-1008 switch is eight. If Telnet is also enabled, the switch can have up to eight Telnet or SSH sessions, in any combination, and one Console session.

**See Also:**
- crypto generate key
- set ip ssh
- set ip ssh server

# set ip telnet

Changes the TCP port number on which a switch listens for Telnet management traffic.

**Caution:** If you change the Telnet port number from a Telnet session, MSS immediately ends the session. To open a new management session, you must Telnet to the switch with the new Telnet port number.

**Syntax: set ip telnet** *port-num*

*port-num* TCP port number.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** The default Telnet port number is 23.

**Access:** Enabled.

**Examples:** The following command changes the Telnet port number on a switch to 5000:

```
DWS-1008# set ip telnet 5000
success: change accepted.
```

**See Also:**
- clear ip telnet
- set ip https server
- set ip telnet server
- show ip https
- show ip telnet

# set ip telnet server

Enables the Telnet server on a DWS-1008 switch.

**Caution:** If you disable the Telnet server, Telnet access to the switch is also disabled.

**Syntax: set ip telnet server {enable | disable}**

**enable** Enables the Telnet server.

**disable** Disables the Telnet server.

**Defaults:** The Telnet server is disabled by default.

**Access:** Enabled.

**Usage:** The maximum number of Telnet sessions supported on a DWS-1008 switch is eight. If SSH is also enabled, the switch can have up to eight Telnet or SSH sessions, in any combination, and one console session.

**Examples:** The following command enables the Telnet server on a DWS-1008 switch:

```
DWS-1008# set ip telnet server enable
success: change accepted.
```

**See Also:**
- clear ip telnet
- set ip https server
- set ip telnet
- show ip https
- show ip telnet


Download from Www.Somanuals.com. All Manuals Search And Download.

# set ntp

Enables or disables the NTP client on a DWS-1008 switch.

**Syntax: set ntp {enable | disable}**

**enable** Enables the NTP client.

**disable** Disables the NTP client.

**Defaults:** The NTP client is disabled by default.

**Access:** Enabled.

**Usage:** If NTP is configured on a system whose current time differs from the NTP server time by more than 10 minutes, convergence of the switch time can take many NTP update intervals. D-link recommends that you set the time manually to the NTP server time before enabling NTP to avoid a significant delay in convergence.

**Examples:** The following command enables the NTP client:

```
DWS-1008# set ntp enable
success: NTP Client enabled
```

**See Also:**
- clear ntp server
- clear ntp update-interval
- set ntp server
- set ntp update-interval
- show ntp

# set ntp server

Configures a DWS-1008 switch to use an NTP server.

**Syntax: set ntp server** *ip-addr*

*ip-addr* IP address of the NTP server, in dotted decimal notation.

**Defaults:** None.

**Access:** Enabled.

**Usage;** You can configure up to three NTP servers. MSS queries all the servers and selects the best response based on the method described in RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis.

To use NTP, you also must enable the NTP client with the **set ntp** command.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command configures a switch to use NTP server 192.168.1.5:

```
DWS-1008# set ntp server 192.168.1.5
```

**See Also:**
- clear ntp server
- clear ntp update-interval
- set ntp
- set ntp update-interval
- show ntp

# set ntp update-interval

Changes how often MSS sends queries to the NTP servers for updates.

**Syntax: set ntp update-interval** *seconds*

| | |
|---|---|
| *seconds* | Number of seconds between queries. You can specify from 16 through 1024 seconds. |

**Defaults:** The default NTP update interval is 64 seconds.

**Access:** Enabled.

**Examples:** The following command changes the NTP update interval to 128 seconds:

```
DWS-1008# set ntp update-interval 128
success: change accepted.
```

**See Also:**
- clear ntp server
- clear ntp update-interval
- set ntp
- set ntp server
- show ntp


Download from Www.Somanuals.com. All Manuals Search And Download.

# set snmp community

Configures a community string for SNMPv1 or SNMPv2c.

**Note:** For SNMPv3, use the **set snmp usm** command to configure an SNMPv3 user. SNMPv3 does not use community strings.

**Syntax: set snmp community name** *comm-string* **access {read-only | read-notify | notify-only | read-write | notify-read-write}**

| | |
|---|---|
| *comm-string* | Name of the SNMP community. Specify between 1 and 32 alphanumeric characters, with no spaces. |
| **read-only** | Allows an SNMP management application using the string to get (read) object values on the switch but not to set (write) them. |
| **read-notify** | Allows an SNMP management application using the string to get object values on the switch but not to set them. The switch can use the string to send notifications. |
| **notify-only** | Allows the switch to use the string to send notifications. |
| **read-write** | Allows an SNMP management application using the string to get and set object values on the switch. |
| **notify-read-write** | Allows an SNMP management application using the string to get and set object values on the switch. The switch also can use the string to send notifications. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** SNMP community strings are passed as clear text in SNMPv1 and SNMPv2c. D-Link recommends that you use strings that cannot easily be guessed by unauthorized users. For example, do not use the well-known strings public and private.

If you are using SNMPv3, you can configure SNMPv3 users to use authentication and to encrypt SNMP data.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command configures the read-write community good_community:

```
DWS-1008# set snmp community read-write good_community
success: change accepted.
```

The following command configures community string *switchmgr1* with access level notify-read-write:

```
DWS-1008# set snmp community name switchmgr1 notify-read-write
success: change accepted.
```

**See Also:**
- clear snmp community
- set ip snmp server
- set snmp notify target
- set snmp notify profile
- set snmp protocol
- set snmp security
- set snmp usm
- show snmp community

# set snmp notify profile

Configures an SNMP notification profile. A notification profile is a named list of all the notification types that can be generated by a switch, and for each notification type, the action to take (drop or send) when an event occurs.

You can configure up to ten notification profiles.

**Syntax: set snmp notify profile {default |** *profile-name***}{drop | send}**
**{***notification-type* **| all}**

| | |
|---|---|
| **default** \| *profile-name* | Name of the notification profile you are creating or modifying. The profile-name can be up to 32 alphanumeric characters long, with no spaces. To modify the default notification profile, specify default. |
| **drop \| send** | Specifies the action that the SNMP engine takes with regard to the notifications you specify with *notification-type* or **all**. |


Download from Www.Somanuals.com. All Manuals Search And Download.

*notification-type* Name of the notification type:

- **APBootTraps**—Generated when an access point boots.
- **ApNonOperStatusTraps**—Generated to indicate an AP radio is nonoperational.
- **ApOperRadioStatusTraps**—Generated when the status of an AP radio changes.
- **APTimeoutTraps**—Generated when an access point fails to respond to the switch.
- **AuthenTraps**—Generated when the switch's SNMP engine receives a bad community string.
- **AutoTuneRadioChannelChangeTraps**—Generated when the RF Auto-Tuning feature changes the channel on a radio.
- **AutoTuneRadioPowerChangeTraps**—Generated when the RFAuto-Tuning feature changes the power setting on a radio.
- **ClientAssociationFailureTraps**—Generated when a client's attempt to associate with a radio fails.
- **ClientAuthorizationSuccessTraps**—Generated when a client is successfully authorized.
- **ClientAuthenticationFailureTraps**—Generated when authentication fails for a client.
- **ClientAuthorizationFailureTraps**—Generated when authorization fails for a client.
- **ClientClearedTraps**—Generated when a client's session is cleared.
- **ClientDeAssociationTraps**—Generated when a client is dissociated from a radio.
- **ClientDot1xFailureTraps**—Generated when a client experiences an 802.1X failure.
- **ClientRoamingTraps**—Generated when a client roams.
- **CounterMeasureStartTraps**—Generated when MSS begins countermeasures against a rogue access point.


Download from Www.Somanuals.com. All Manuals Search And Download.

- **CounterMeasureStopTraps**—Generated when MSS stops countermeasures against a rogue access point.
- **DAPConnectWarningTraps**—Generated when a Distributed AP whose fingerprint has not been configured in MSS establishes a management session with the switch.
- **DeviceFailTraps**—Generated when an event with an Alert severity occurs.
- **DeviceOkayTraps**—Generated when a device returns to its normal state.
- **LinkDownTraps**—Generated when the link is lost on a port.
- **LinkUpTraps**—Generated when the link is detected on a port.
- **MichaelMICFailureTraps**—Generated when two Michael message integrity code (MIC) failures occur within 60 seconds, triggering Wi-Fi Protected Access (WPA) countermeasures.
- **PoEFailTraps**—Generated when a serious PoE problem, such as a short circuit, occurs.
- **RFDetectAdhocUserTraps**—Generated when MSS detects an ad-hoc user.
- **RFDetectRogueAPTraps**—Generated when MSS detects a rogue access point.
- **RFDetectRogueDisappearTraps**—Generated when a rogue access point is no longer being detected.
- **RFDetectClientViaRogueWiredAPTraps**—Generated when MSS detects, on the wired part of the network, the MAC address of a wireless client associated with a third-party AP.
- **RFDetectDoSPortTraps**—Generated when MSS detects an associate request flood, reassociate request flood, or disassociate request flood.
- **RFDetectDoSTraps**—Generated when MSS detects a DoS attack other than an associate request flood, reassociate request flood, or disassociate request flood.
- **RFDetectInterferingRogueAPTraps**—Generated when an interfering device is detected.
- **RFDetectInterferingRogueDisappearTraps**—Generated when an interfering device is no longer detected.
- **RFDetectSpoofedMacAPTraps**—Generated when MSS detects a wireless packet with the source MAC address of a D-Link AP, but without the spoofed AP's signature (fingerprint).
- **RFDetectSpoofedSsidAPTraps**—Generated when MSS detects beacon frames for a valid SSID, but sent by a rogue AP.
- **RFDetectUnAuthorizedAPTraps**—Generated when MSS detects the MAC address of an AP that is on the attack list.
- **RFDetectUnAuthorizedOuiTraps**—Generated when a wireless device that is not on the list of permitted vendors is detected.
- **RFDetectUnAuthorizedSsidTraps**—Generated when an SSID that is not on the permitted SSID list is detected.


Download from Www.Somanuals.com. All Manuals Search And Download.

*all* Sends or drops all notifications.

**Defaults:** A default notification profile (named default) is already configured in MSS. All notifications in the default profile are dropped by default.

**Access:** Enabled.

**Examples:** The following command changes the action in the default notification profile from drop to send for all notification types:

```
DWS-1008# set snmp notify profile default send all
success: change accepted.
```

The following commands create notification profile *snmpprof_rfdetect*, and change the action to send for all RF detection notification types:

```
DWS-1008# set snmp notify profile snmpprof_rfdetect send RFDetectAdhocUserTraps
success: change accepted.

DWS-1008# set snmp notify profile snmpprof_rfdetect send
RFDetectClientViaRogueWiredAPTraps
success: change accepted.

DWS-1008# set snmp notify profile snmpprof_rfdetect send RFDetectDoSTraps
success: change accepted.

DWS-1008# set snmp notify profile snmpprof_rfdetect send RFDetectAdhocUserTraps
success: change accepted.

DWS-1008# set snmp notify profile snmpprof_rfdetect send
RFDetectInterferingRogueAPTraps
success: change accepted.

DWS-1008# set snmp notify profile snmpprof_rfdetect send
RFDetectInterferingRogueDisappearTraps
success: change accepted.

DWS-1008# set snmp notify profile snmpprof_rfdetect send RFDetectRogueAPTraps
success: change accepted.

DWS-1008# set snmp notify profile snmpprof_rfdetect send
RFDetectRogueDisappearTraps
success: change accepted.

DWS-1008# set snmp notify profile snmpprof_rfdetect send
RFDetectSpoofedMacAPTraps
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

DWS-1008# **set snmp notify profile snmpprof_rfdetect send RFDetectSpoofedSsidAPTraps**
success: change accepted.

DWS-1008# **set snmp notify profile snmpprof_rfdetect send RFDetectUnAuthorizedAPTraps**
success: change accepted.

DWS-1008# **set snmp notify profile snmpprof_rfdetect send RFDetectUnAuthorizedOuiTraps**
success: change accepted.

DWS-1008# **set snmp notify profile snmpprof_rfdetect send RFDetectUnAuthorizedSsidTraps**
success: change accepted.

# set snmp notify target

Configures a notification target for notifications from SNMP.

A notification target is a remote device to which MSS sends SNMP notifications. You can configure the MSS SNMP engine to send confirmed notifications (informs) or unconfirmed notifications (traps). Some of the command options differ depending on the SNMP version and the type of notification you specify. You can configure up to 10 notification targets.

**SNMPv3 with Informs**

To configure a notification target for informs from SNMPv3, use the following command:

**Syntax: set snmp notify target** *target-num ip-addr* **[***:udp-port-number***]**
**usm inform user** *username* **snmp-engine-id {ip | hex** *hex-string***}**
**[profile** *profile-name***] [security {unsecured | authenticated | encrypted}]**
**[retries** *num***] [timeout** *num***]**

| | |
|---|---|
| *target-num* | ID for the target. This ID is local to the switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10. |
| *ip-addr[:udp-port-number]* | IP address of the server. You also can specify the UDP port number to send notifications to. |
| *username* | USM username. This option is applicable only when the SNMP version is usm. If the user will send informs rather than traps, you also must specify the snmp-engine-id of the target. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| **snmp-engine-id {ip \| hex** *hex-string***}** | SNMP engine ID of the target. Specify ip if the target's SNMP engine ID is based on its IP address. If the target's SNMP engine ID is a hexadecimal value, use **hex** *hex-string* to specify the value. |
| **profile** *profile-name* | Notification profile this SNMP user will use to specify the notification types to send or drop. |
| **security {unsecured \| authenticated \| encrypted}** | Specifies the security level, and is applicable only when the SNMP version is usm:<br>• **unsecured**—Message exchanges are not authenticated, nor are they encrypted. This is the default.<br>• **authenticated**—Message exchanges are authenticated, but are not encrypted.<br>• **encrypted**—Message exchanges are authenticated and encrypted. |
| retries num | Specifies the number of times the MSS SNMP engine will resend a notification that has not been acknowledged by the target. You can specify from 0 to 3 retries. |
| timeout num | Specifies the number of seconds MSS waits for acknowledgement of a notification. You can specify from 1 to 5 seconds. |

**SNMPv3 with Traps**

To configure a notification target for traps from SNMPv3, use the following command:

**Syntax: set snmp notify target** *target-num ip-addr***[***:udp-port-number***]**
**usm trap user** *username* **[profile** *profile-name***]**
**[security {unsecured | authenticated | encrypted}]**

| | |
|---|---|
| *target-num* | ID for the target. This ID is local to the switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10. |
| *ip-addr[:udp-port-number]* | IP address of the server. You also can specify the UDP port number to send notifications to. |
| *username* | USM username. This option is applicable only when the SNMP version is usm. |
| **profile** *profile-name* | Notification profile this SNMP user will use to specify the notification types to send or drop. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| **security {unsecured \| authenticated \| encrypted}** | Specifies the security level, and is applicable only when applicable only when the SNMP version is usm:<br>• **unsecured**—Message exchanges are not authenticated, nor are they encrypted. This is the default.<br>• **authenticated**—Message exchanges are authenticated, but are not encrypted.<br>• **encrypted**—Message exchanges are authenticated and encrypted. |

**SNMPv2c with Informs**

To configure a notification target for informs from SNMPv2c, use the following command:

**Syntax: set snmp notify target** *target-num ip-addr***[***:udp-port-number***] v2c** *community-string* **inform [profile** *profile-name***] [retries** *num***] [timeout** *num***]**

| | |
|---|---|
| *target-num* | ID for the target. This ID is local to the switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10. |
| *ip-addr[:udp-port-number]* | IP address of the server. You also can specify the UDP port number to send notifications to. |
| *community-string* | Community string. |
| **profile** *profile-name* | Notification profile this SNMP user will use to specify the notification types to send or drop. |
| **retries** *num* | Specifies the number of times the MSS SNMP engine will resend a notification that has not been acknowledged by the target. You can specify from 0 to 3 retries. |
| **timeout** *num* | Specifies the number of seconds MSS waits for acknowledgement of a notification. You can specify from 1 to 5 seconds. |

**SNMPv2c with Traps**

To configure a notification target for traps from SNMPv2c, use the following command:

**Syntax: set snmp notify target** *target-num ip-addr***[***:udp-port-number***]**
**v2c** *community-string* **trap [profile** *profile-name***]**


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| *target-num* | ID for the target. This ID is local to the switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10. |
| *ip-addr[:udp-port-number]* | IP address of the server. You also can specify the UDP port number to send notifications to. |
| *community-string* | Community string. |
| **profile** *profile-name* | Notification profile this SNMP user will use to specify the notification types to send or drop. |

**SNMPv1 with Traps**

To configure a notification target for traps from SNMPv1, use the following command:

**Syntax: set snmp notify target** *target-num ip-addr* **[***:udp-port-number***]**
**v1** *community-string* **[profile** *profile-name***]**

| | |
|---|---|
| *target-num* | ID for the target. This ID is local to the switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10. |
| *ip-addr[:udp-port-number]* | IP address of the server. You also can specify the UDP port number to send notifications to. |
| *community-string* | Community string. |
| **profile** *profile-name* | Notification profile this SNMP user will use to specify the notification types to send or drop. |

**Defaults:** The default UDP port number on the target is 162. The default minimum required security level is unsecured. The default number of retries is 0 and the default timeout is 2 seconds.

**Access:** Enabled.

**Usage:** The inform or trap option specifies whether the MSS SNMP engine expects the target to acknowledge notifications sent to the target by the switch. Use inform if you want acknowledgements. Use trap if you do not want acknowledgements. The inform option is applicable to SNMP version v2c or usm only.

**Examples:** The following command configures a notification target for acknowledged notifications:

```
DWS-1008# set snmp notify target 1 10.10.40.9 usm inform user securesnmpmgr1
snmp-engine-id ip
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

This command configures target 1 at IP address 10.10.40.9. The target's SNMP engine ID is based on its address. The MSS SNMP engine will send notifications based on the default profile, and will require the target to acknowledge receiving them.

The following command configures a notification target for unacknowledged notifications:

```
DWS-1008# set snmp notify target 2 10.10.40.10 v1 trap
success: change accepted.
```

**See Also:**
- clear snmp notify target
- set ip snmp server
- set snmp community
- set snmp notify profile
- set snmp protocol
- set snmp security
- set snmp usm
- show snmp notify target

# set snmp protocol

Enables an SNMP protocol. MSS supports SNMPv1, SNMPv2c, and SNMPv3.

**Syntax: set snmp protocol {v1 | v2c | usm | all} {enable | disable}**

| | |
|---|---|
| **v1** | SNMPv1 |
| **v2c** | SNMPv2c |
| **usm** | SNMPv3 (with the user security model) |
| **all** | Enables all supported versions of SNMP. |
| **enable** | Enables the specified SNMP version(s). |
| **disable** | Disables the specified SNMP version(s). |

**Defaults:** All SNMP versions are disabled by default.

**Access:** Enabled.

**Usage:** SNMP requires the switch's system IP address to be set. SNMP will not work without the system IP address. You also must enable the SNMP service using the set ip snmp server command.

**Examples:** The following command enables all SNMP versions:

```
DWS-1008# set snmp protocol all enable
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set snmp security

Sets the minimum level of security MSS requires for SNMP message exchanges.

**Syntax: set snmp security {unsecured | authenticated | encrypted | auth-req-unsec-notify}**

| | |
|---|---|
| **unsecured** | SNMP message exchanges are not secure. This is the only value supported for SNMPv1 and SNMPv2c. |
| **authenticated** | SNMP message exchanges are authenticated but are not encrypted. |
| **encrypted** | SNMP message exchanges are authenticated and encrypted. |
| **auth-req-unsecnotify** | SNMP message exchanges are authenticated but are not encrypted, and notifications are neither authenticated nor encrypted. |

**Defaults:** By default, MSS allows nonsecure (unsecured) SNMP message exchanges.

**Access:** Enabled.

**Usage:** SNMPv1 and SNMPv2c do not support authentication or encryption. If you plan to use SNMPv1 or SNMPv2c, leave the minimum level of SNMP security set to unsecured.

**Examples:** The following command sets the minimum level of SNMP security allowed to authentication and encryption:

```
DWS-1008# set snmp security encrypted
success: change accepted.
```

**See Also:**
- set ip snmp server
- set snmp community
- set snmp notify target
- set snmp notify profile
- set snmp protocol
- set snmp usm
- show snmp status


Download from Www.Somanuals.com. All Manuals Search And Download.

# set snmp usm

Creates a USM user for SNMPv3.

**Note:** This command does not apply to SNMPv1 or SNMPv2c. For these SNMP versions, use the set snmp community command to configure community strings.

**Syntax: set snmp usm** *usm-username*
**snmp-engine-id {ip** *ip-addr* **| local | hex** *hex-string***}**
**access {read-only | read-notify | notify-only | read-write | notify-read-write}**
**auth-type {none | md5 | sha} {auth-pass-phrase** *string* **| auth-key** *hex-string***}**
**encrypt-type {none | des | 3des | aes}**
**{encrypt-pass-phrase** *string* **| encrypt-key** *hex-string***}**

| | |
|---|---|
| *usm-username* | Name of the SNMPv3 user. Specify between 1 and 32 alphanumeric characters, with no spaces. |
| snmp-engine-id {ip ip-addr \| local \| hex hex-string} | Specifies a unique identifier for the SNMP engine. To send informs, you must specify the engine ID of the inform receiver. To send traps and to allow get and set operations and so on, specify local as the engine ID.<br>• hex hex-string—ID is a hexadecimal string.<br>• ip ip-addr—ID is based on the IP address of the station running the management application. Enter the IP address of the station. MSS calculates the engine ID based on the address.<br>• local—Uses the value computed from the switch's system IP address. |
| **access {read-only \| read-notify \| notify-only \| read-write \| notify-read-write}** | Specifies the access level of the user:<br>• read-only—An SNMP management application using the string can get (read) object values on the switch but cannot set (write) them.<br>• read-notify—An SNMP management application using the string can get object values on the switch but cannot set them. The switch can use the string to send notifications.<br>• notify-only—The switch can use the string to send notifications.<br>• read-write—An SNMP management application using the string can get and set object values on the switch.<br>• notify-read-write—An SNMP management application using the string can get and set object values on the switch. The switch can use the string to send notifications. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| **auth-type {none \| md5 \| sha} {auth-pass-phrase** *string* **\| auth-key** *hex-string***}** | Specifies the authentication type used to authenticate communications with the remote SNMP engine. You can specify one of the following:<br>• none—No authentication is used.<br>• md5—Message-digest algorithm 5 is used.<br>• sha—Secure Hashing Algorithm (SHA) is used.<br><br>If the authentication type is md5 or sha, you can specify a passphrase or a hexadecimal key.<br>• To specify a passphrase, use the auth-pass-phrase string option. The string can be from 8 to 32 alphanumeric characters long, with no spaces.<br>• To specify a key, use the auth-key hex-string option. |
| **encrypt-type {none \| des \| 3des \| aes} {encrypt-pass-phrase** *string* **\| encrypt-key** *hex-string***}** | Specifies the encryption type used for SNMP traffic. You can specify one of the following:<br>• none—No encryption is used. This is the default.<br>• des—Data Encryption Standard (DES) encryption is used.<br>• 3des—Triple DES encryption is used.<br>• aes—Advanced Encryption Standard (AES) encryption is used.<br><br>If the encryption type is des, 3des, or aes, you can specify a passphrase or a hexadecimal key.<br>• To specify a passphrase, use the encrypt-pass-phrase string option. The string can be from 8 to 32 alphanumeric characters long, with no spaces.<br>• To specify a key, use the encrypt-key hex-string option. |

**Defaults:** No SNMPv3 users are configured by default. When you configure an SNMPv3 user, the default access is read-only, and the default authentication and encryption types are both none.

**Access:** Enabled.

**Examples:** The following command creates USM user *snmpmgr1*, associated with the local SNMP engine ID. This user can send traps to notification receivers.

```
DWS-1008# set snmp usm snmpmgr1 snmp-engine-id local
success: change accepted.
```

The following command creates USM user *securesnmpmgr1*, which uses SHA authentication and 3DES encryption with passphrases. This user can send informs to the notification receiver that has engine ID 192.168.40.2.

```
DWS-1008# set snmp usm securesnmpmgr1 snmp-engine-id ip 192.168.40.2 auth-
type sha auth-pass-phrase myauthpword encrypt-type 3des encrypt-pass-phrase
mycryptpword
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set summertime

Offsets the real-time clock of a DWS-1008 switch by +1 hour and returns it to standard time for daylight savings time or a similar summertime period that you set.

**Syntax: set summertime** *summer-name* **[start** *week weekday month hour min*
**end** *week weekday month hour min***]**

| | |
|---|---|
| *summer-name* | Name of up to 32 alphanumeric characters that describes the summertime offset. You can use a standard name or any name you like. |
| **start** | Start of the time change period. |
| *week* | Week of the month to start or end the time change. Valid values are first, second, third, fourth, or last. |
| *weekday* | Day of the week to start or end the time change. Valid values are sun, mon, tue, wed, thu, fri, and sat. |
| *month* | Month of the year to start or end the time change. Valid values are jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, and dec. |
| *hour* | Hour to start or end the time change—a value between 0 and 23 on the 24-hour clock. |
| *min* | Minute to start or end the time change—a value between 0 and 59. |
| **end** | End of the time change period. |

**Defaults:** If you do not specify a start and end time, the system implements the time change starting at 2:00 a.m. on the first Sunday in April and ending at 2:00 a.m. on the last Sunday in October, according to the North American standard.

**Access:** Enabled.

**Usage:** You must first set the time zone with the **set timezone** command for the offset to work properly without the start and end values. Configure summertime before you set the time and date. Otherwise, summertime's adjustment of the time will make the time incorrect, if the date is within the summertime period.

**Examples:** To enable summertime and set the summertime time zone to PDT (Pacific Daylight Time), type the following command:

```
DWS-1008# set summertime PDT
success: change accepted
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set system ip-address

Configures the system IP address. The system IP address determines the interface or source IP address MSS uses for system tasks, including the following:

- Topology reporting for dual-homed access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

**Syntax: set system ip-address** *ip-addr*

| | |
|---|---|
| *ip-addr* | IP address, in dotted decimal notation. The address must be configured on one of the switch's VLANs. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** You must use an address that is configured on one of the switch's VLANs.

To display the system IP address, use the **show system** command.

**Examples:** The following commands configure an IP interface on VLAN *taupe* and configure the interface to be the system IP address:

```
DWS-1008# set interface taupe ip 10.10.20.20/24
success: set ip address 10.10.20.20 netmask 255.255.255.0 on vlan taupe

DWS-1008# set system ip-address 10.10.20.20
success: change accepted.
```

**See Also:**
- clear system ip-address
- set interface
- show system


Download from Www.Somanuals.com. All Manuals Search And Download.

# set timedate

Sets the time of day and date on the DWS-1008 switch.

**Syntax: set timedate {date** *mmm dd yyyy* **[time** *hh:mm:ss***]}**

| | |
|---|---|
| **date** *mmm dd yyyy* | System date:<br>• mmm—month.<br>• dd—day.<br>• yyyy—year. |
| **time** *hh:mm:ss* | System time, in hours, minutes, and seconds. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** The day of week is automatically calculated from the day you set. The time displayed by the CLI after you type the command might be slightly later than the time you enter due to the interval between when you press Enter and when the CLI reads and displays the new time and date.

Configure summertime before you set the time and date. Otherwise, summertime's adjustment of the time will make the time incorrect, if the date is within the summertime period.

**Examples:** The following command sets the date to March 13, 2003 and time to 11:11:12:

```
DWS-1008# set timedate date feb 29 2004 time 23:58:00
Time now is: Sun Feb 29 2004, 23:58:02 PST
```

# set timezone

Sets the number of hours, and optionally the number of minutes, that the switch's real-time clock is offset from Coordinated Universal Time (UTC). These values are also used by Network Time Protocol (NTP), if it is enabled.

**Syntax: set timezone** *zone-name* **{**-*hours* **[***minutes***]}**

| | |
|---|---|
| *zone-name* | Time zone name of up to 32 alphabetic characters. You can use a standard name or any name you like. |
| - | Minus time to indicate hours (and minutes) to be subtracted from UTC. Otherwise, hours and minutes are added by default. |
| *hours* | Number of hours to add or subtract from UTC. |
| *minutes* | Number of minutes to add or subtract from UTC. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** If this command is not used, then the default time zone is UTC.

**Access:** Enabled.

**Examples:** To set the time zone for Pacific Standard Time (PST), type the following command:

DWS-1008# **set timezone PST -8**
Timezone is set to 'PST', offset from UTC is -8:0 hours.

**See Also:**
- clear summertime
- clear timezone
- set summertime
- set timedate
- show summertime
- show timedate
- show timezone

# show arp

Displays the ARP table.

**Syntax: show arp [***ip-addr***]**

*ip-addr* IP address.

**Defaults:** If you do not specify an IP address, the whole ARP table is displayed.

**Access:** All.

**Examples:** The following command displays ARP entries:

```
DWS-1008# show arp
ARP aging time: 1200 seconds
Host          HW Address        VLAN        Type        State
-------------------------------------------------------------------------------------
10.5.4.51     00:0b:0e:02:76:f5  1           DYNAMIC     RESOLVED
10.5.4.53     00:0b:0e:02:76:f7  1           LOCAL       RESOLVED
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields in this display.

| Field | Description |
|---|---|
| ARP aging time | Number of seconds a dynamic entry can remain unused before MSS removes the entry from the ARP table. |
| Host | IP address, hostname, or alias. |
| HW Address | MAC address mapped to the IP address, hostname, or alias. |
| VLAN | VLAN the entry is for. |
| Type | Entry type:<br>• **DYNAMIC**—Entry was learned from network traffic and ages out if unused for longer than the ARP aging timeout.<br>• **LOCAL**—Entry for the switch MAC address. Each VLAN has one local entry for the switch MAC address.<br>• **PERMANENT**—Entry does not age out and remains in the configuration even following a reboot.<br>• **STATIC**—Entry does not age out but is removed after a reboot. |
| State | Entry state:<br>• **RESOLVING**—MSS sent an ARP request for the entry and is waiting for the reply.<br>• **RESOLVED**—Entry is resolved. |

**See Also:**
• set arp
• set arp agingtime

# show dhcp-client

Displays DHCP client information for all VLANs.

**Syntax: show dhcp-client**

**Defaults:** None.

**Access:** All.

**Examples:** The following command displays DHCP client information:

```
DWS-1008# show dhcp-client
Interface:              corpvlan(4)
Configuration Status:   Enabled
DHCP State:             IF_UP
Lease Allocation:       65535 seconds
Lease Remaining:        65532 seconds
IP Address:             10.3.1.110
Subnet Mask:            255.255.255.0
Default Gateway:        10.3.1.1
DHCP Server:            10.3.1.4
DNS Servers:            10.3.1.29
DNS Domain Name:        mycorp.com
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Interface | VLAN name and number. |
| Configuration Status | Status of the DHCP client on this VLAN:<br>• Enabled<br>• Disabled |
| DHCP State | State of the IP interface:<br>• IF_UP<br>• IF_DOWN |
| Lease Allocation | Duration of the address lease. |
| Lease Remaining | Number of seconds remaining before the address lease expires. |
| IP Address | IP address received from the DHCP server. |
| Subnet Mask | Network mask of the IP address received from the DHCP server. |
| Default Gateway | Default router (gateway) IP address received from the DHCP server. If the address is 0.0.0.0, the server did not provide an address. |
| DHCP Server | IP address of the DHCP server. |
| DNS Servers | DNS server IP address(es) received from the DHCP server. |
| DNS Domain Name | Default DNS domain name received from the DHCP server. |

**See Also:**
• set interface dhcp-client

# show dhcp-server

Displays MSS DHCP server information.

**Syntax: show dhcp-server [interface** *vlan-id***] [verbose]**

**interface** *vlan-id* Displays the IP addresses leased by the specified VLAN.

**verbose** Displays configuration and status information for the MSS DHCP server.

**Defaults:** None.

**Access:** All.

**Examples:** The following command displays the addresses leased by the MSS DHCP server:

```
DWS-1008# show dhcp-server
VLAN  Name       Address      MAC                Lease Remaining (sec)
-------------------------------------------------------------------------------------------------
1     default    10.10.20.2   00:01:02:03:04:05  12345
1     default    10.10.20.3   00:01:03:04:06:07  2103
2     red-vlan   192.168.1.5  00:01:03:04:06:08  102
2     red-vlan   192.168.1.7  00:01:03:04:06:09  16789
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The following command displays configuration and status information for each VLAN on which the DHCP server is configured:

```
DWS-1008# show dhcp-server verbose
Interface:              0 (Direct AP)
Status:                 UP
Address Range:          10.0.0.1-10.0.0.253

Interface:              default(1)
Status:                 UP
Address Range:          10.10.20.2-10.10.20.254
Hardware Address:       00:01:02:03:04:05
State:                  BOUND
Lease Allocation:       43200 seconds
Lease Remaining:        12345 seconds
IP Address:             10.10.20.2
Subnet Mask:            255.255.255.0
Default Router:         10.10.20.1
DNS Servers:            10.10.20.4 10.10.20.5
DNS Domain Name:        mycorp.com
```

The table below displays output for **show dhcp-server:**

| Field | Description |
|---|---|
| VLAN | VLAN number. |
| Name | VLAN name. |
| Address | IP address leased by the server. |
| MAC Address | MAC address of the device that holds the lease for the address. |
| Lease Remaining | Number of seconds remaining before the address lease expires. |

The table below displays the output for **show dhcp-server verbose:**

| Field | Description |
|---|---|
| Interface | VLAN name and number. |
| Status | Status of the interface:<br>• UP<br>• DOWN |
| Address Range | Range from which the server can lease addresses. |
| Hardware Address | MAC address of the DHCP client. |
| State | State of the address lease:<br>• SUSPEND—MSS is checking for the presence of another DHCP server on the subnet. This is the initial state of the MSS DHCP server. The MSS DHCP server remains in this state if another DHCP server is detected.<br>• CHECKING—MSS is using ARP to verify whether the address is available.<br>• OFFERING—MSS offered the address to the client and is waiting for the client to send a DHCPREQUEST for the address.<br>• BOUND—The client accepted the address.<br>• HOLDING—The address is already in use and is therefore unavailable. |
| Lease Allocation | Duration of the address lease, in seconds. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| Lease Remaining | Number of seconds remaining before the address lease expires. |
| IP Address | IP address leased to the client. |
| Subnet Mask | Network mask of the IP address leased to the client. |
| Default Router | Default router IP address included in the DHCP Offer to the client. |
| DNS Servers | DNS server IP address(es) included in the DHCP Offer to the client. |
| DNS Domain Name | Default DNS domain name included in the DHCP Offer to the client. |

# show interface

Displays the IP interfaces configured on the switch.

**Syntax: show interface [***vlan-id***]**

*vlan-id* VLAN name or number.

**Defaults:** If you do not specify a VLAN ID, interfaces for all VLANs are displayed.

**Access:** All.

**Usage:** You can assign one IP interface to each VLAN. If an interface is already configured on the VLAN you specify, this command replaces the interface. If you replace an interface that is in use as the system IP address, replacing the interface can interfere with system tasks that use the system IP address, including the following:

- Topology reporting for dual-homed access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

**Examples:** The following command configures IP interface 10.10.10.10/24 on VLAN default:

```
DWS-1008# set interface default ip 10.10.10.10/24
success: set ip address 10.10.10.10 netmask 255.255.255.0 on vlan default
```

The following command configures IP interface 10.10.20.10 255.255.255.0 on VLAN mauve:

```
DWS-1008# set interface mauve ip 10.10.20.10 255.255.255.0
success: set ip address 10.10.20.10 netmask 255.255.255.0 on vlan mauve
```

**See Also:**
- clear interface
- set interface status
- show interface


Download from Www.Somanuals.com. All Manuals Search And Download.

# set interface dhcp-client

Configures the DHCP client on a VLAN, to allow the VLAN to obtain its IP interface from a DHCP server.

**Syntax: set interface** *vlan-id* **ip dhcp-client {enable | disable}**

*vlan-id* VLAN name or number.

**enable** Enables the DHCP client on the VLAN.

**disable** Disables the DHCP client on the VLAN.

**Defaults:** The DHCP client is disabled by default.

**Access:** Enabled.

**Usage:** You can enable the DHCP client on one VLAN only. You can configure the DHCP client on more than one VLAN, but the client can be active on only one VLAN.

MSS also has a configurable DHCP server. You can configure a DHCP client and DHCP server on the same VLAN, but only the client or the server can be enabled. The DHCP client and DHCP server cannot both be enabled on the same VLAN at the same time.

**Examples:** The following command enables the DHCP client on VLAN *corpvlan*:

```
DWS-1008# set interface corpvlan ip dhcp-client enable
success: change accepted.
```

**See Also:**
- clear interface
- show dhcp-client
- show interface


Download from Www.Somanuals.com. All Manuals Search And Download.

# set interface dhcp-server

Configures the MSS DHCP server.

**Note:** Use of the MSS DHCP server to allocate client addresses is intended for temporary, demonstration deployments and not for production networks. D-Link recommends that you do not use the MSS DHCP server to allocate client addresses in a production network.

**Syntax: set interface** *vlan-id* **ip dhcp-server [enable | disable] [start** *ip-addr1*
**stop** *ip-addr2***] [dns-domain** *domain-name***] [primary-dns** *ip-addr*
**[secondary-dns** *ip-addr***]] [default-router** *ip-addr***]**

| | |
|---|---|
| *vlan-id* | VLAN name or number. |
| **enable** | Enables the DHCP server. |
| **disable** | Disables the DHCP server. |
| **start** *ip-addr1* | Specifies the beginning address of the address range (also called the address pool). |
| **stop** *ip-addr2* | Specifies the ending address of the address range. |
| **dns-domain** *domain-name* | Name of the DHCP client's default DNS domain. |
| **primary-dns** *ip-addr* **[secondary-dns** *ip-addr***]** | IP addresses of the DHCP client's DNS servers. |
| **default-router** *ip-addr* | IP address of the DHCP client's default router. |

**Defaults:** The DHCP server is enabled and cannot be disabled for directly connected APs. The DHCP server is disabled by default for any other use.

**Access:** Enabled.

**Usage:** By default, all addresses except the host address of the VLAN, the network broadcast address, and the subnet broadcast address are included in the range. If you specify the range, the start address must be lower than the stop address, and all addresses must be in the same subnet. The IP interface of the VLAN must be within the same subnet but is not required to be within the range.


Download from Www.Somanuals.com. All Manuals Search And Download.

Specification of the DNS domain name, DNS servers, and default router are optional. If you omit one or more of these options, the MSS DHCP server uses oath values configured elsewhere on the switch:

- **DNS domain name**—If this option is not set with the set interface dhcp-server command's dns-domain option, the MSS DHCP server uses the value set by the set ip dns domain command.
- **DNS servers**—If these options are not set with the set interface dhcp-server command's primary-dns and secondary-dns options, the MSS DHCP server uses the values set by the set ip dns server command.
- **Default router**—If this option is not set with the set interface dhcp-server command's default-router option, the MSS DHCP server can use the value set by the set ip route command. A default route configured by set ip route can be used if the route is in the DHCP client's subnet. Otherwise, the MSS DHCP server does not specify a router address.

**Examples:** The following command enables the DHCP server on VLAN *red-vlan* to serve addresses from the 192.168.1.5 to 192.168.1.25 range:

```
DWS-1008# set interface red-vlan ip dhcp-server enable start 192.168.1.5 stop
192.168.1.25
success: change accepted.
```

**See Also:**
- set ip dns domain
- set ip dns server
- show dhcp-server

# set interface status

Administratively disables or reenables an IP interface.

**Syntax: set interface** *vlan-id* **status {up | down}**

| | |
|---|---|
| *vlan-id* | VLAN name or number. |
| **up** | Enables the interface. |
| **down** | Disables the interface. |

**Defaults:** IP interfaces are enabled by default.

**Access:** Enabled.

**Examples:** The following command disables the IP interface on VLAN *mauve*:

```
DWS-1008# set interface mauve status down
success: set interface mauve to down
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set ip alias

Configures an alias, which maps a name to an IP address. You can use aliases as shortcuts in CLI commands.

**Syntax: set ip alias** *name ip-addr*

*name* String of up to 32 alphanumeric characters, with no spaces.

*ip-addr* IP address in dotted decimal notation.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command configures the alias *HR1* for IP address 192.168.1.2:

```
DWS-1008# set ip alias HR1 192.168.1.2
success: change accepted.
```

**See Also:**
- clear ip alias
- show ip alias

# set ip dns

Enables or disables DNS on a DWS-1008 switch.

**Syntax: set ip dns {enable | disable}**

**enable** Enables DNS.

**disable** Disables DNS.

**Defaults:** DNS is disabled by default.

**Access:** Enabled.

**Examples:** The following command enables DNS on a DWS-1008 switch:

```
DWS-1008# set ip dns enable
Start DNS Client
```

**See Also:**
- clear ip dns domain
- clear ip dns server
- set ip dns domain
- set ip dns server
- show ip dns


Download from Www.Somanuals.com. All Manuals Search And Download.

# set ip dns domain

Configures a default domain name for DNS queries. The switch appends the default domain name to domain names or hostnames you enter in commands.

**Syntax: set ip dns domain** *name*

*name* Domain name of between 1 and 64 alphanumeric characters with no spaces (for example, example.org).

**Defaults:** None.

**Access:** Enabled.

**Usage:** To override the default domain name when entering a hostname in a CLI command, enter a period at the end of the hostname. For example, if the default domain name is example.com, enter chris. if the fully qualified hostname is chris and not chris.example.com.

Aliases take precedence over DNS. When you enter a hostname, MSS checks for an alias with that name first, before using DNS to resolve the name.

**Examples:** The following command configures the default domain name example.com:

```
DWS-1008# set ip dns domain example.com
Domain name changed
```

**See Also:**
- clear ip dns domain
- clear ip dns server
- set ip dns
- set ip dns server
- show ip dns

# set ip dns server

Specifies a DNS server to use for resolving hostnames you enter in CLI commands.

**Syntax: set ip dns server** *ip-addr* **{primary | secondary}**

*ip-addr* IP address of a DNS server, in dotted decimal or CIDR notation.

**primary** Makes the server the primary server, which MSS always consults first for resolving DNS queries.

**secondary** Makes the server a secondary server. MSS consults a secondary server only if the primary server does not reply.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** Enabled.

**Usage:** You can configure a switch to use one primary DNS server and up to five secondary DNS servers.

**Examples:** The following commands configure a switch to use a primary DNS server and two secondary DNS servers:

```
DWS-1008# set ip dns server 10.10.10.50/24 primary
success: change accepted.

DWS-1008# set ip dns server 10.10.20.69/24 secondary
success: change accepted.

DWS-1008# set ip dns server 10.10.30.69/24 secondary
success: change accepted.
```

**See Also:**
- clear ip dns domain
- clear ip dns server
- set ip dns
- set ip dns domain
- show ip dns

# set ip https server

Enables the HTTPS server on a DWS-1008 switch. The HTTPS server is required for Web View access to the switch.

**Caution:** If you disable the HTTPS server, Web View access to the switch is disabled.

**Syntax: set ip https server {enable | disable}**

**enable** Enables the HTTPS server.

**disable** Disables the HTTPS server.

**Defaults:** The HTTPS server is disabled by default.

**Access:** Enabled.

**Examples:** The following command enables the HTTPS server on a switch:

```
DWS-1008# set ip https server enable
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set ip route

Adds a static route to the IP route table.

**Syntax: set ip route {default |** *ip-addr mask* **|** *ip-addr/mask-length***}** *default-router metric*

| | |
|---|---|
| **default** | Default route. A DWS-1008 switch uses the default route if an explicit route is not available for the destination.<br><br>**Note:** default is an alias for IP address 0.0.0.0/0. |
| *ip-addr mask* | IP address and subnet mask for the route destination, in dotted decimal notation (for example, 10.10.10.10 255.255.255.0). |
| *ip-addr/mask-length* | IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24). |
| *default-router* | IP address, DNS hostname, or alias of the next-hop router. |
| *metric* | Cost for using the route. You can specify a value from 0 through 2,147,483,647. Lower-cost routes are preferred over higher-cost routes. |

**Access:** Enabled.

**Usage:** MSS can use a static route only if a direct route in the route table resolves the static route. MSS adds routes with next-hop types Local and Direct when you add an IP interface to a VLAN, if the VLAN is up. If one of these added routes can resolve the static route, MSS can use the static route.

Before you add a static route, use the show interface command to verify that the switch has an IP interface in the same subnet as the route's next-hop router. If not, the VLAN:Interface field of the show ip route command output shows that the route is down.

You can configure a maximum of 4 routes per destination. This includes default routes, which have destination 0.0.0.0/0. Each route to a given destination must have a unique router address. When the route table contains multiple default or explicit routes to the same destination, MSS uses the route with the lowest cost. If two or more routes to the same destination have the lowest cost, MSS selects the first route in the route table.

When you add multiple routes to the same destination, MSS groups the routes and orders them from lowest cost at the top of the group to highest cost at the bottom of the group. If you add a new route that has the same destination and cost as a route already in the table, MSS places the new route at the top of the group of routes with the same cost.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Example:** The following command adds a default route that uses default router 10.5.4.1 and gives the route a cost of 1:

```
DWS-1008# set ip route default 10.5.4.1 1
success: change accepted.
```

The following commands add two default routes, and configure MSS to always use the route through 10.2.4.69 when the switch interface to that default router is up:

```
DWS-1008# set ip route default 10.2.4.69 1
success: change accepted.

DWS-1008# set ip route default 10.2.4.17 2
success: change accepted.
```

The following command adds an explicit route from a switch to any host on the 192.168.4.x subnet through the local router 10.5.4.2, and gives the route a cost of 1:

```
DWS-1008# set ip route 192.168.4.0 255.255.255.0 10.5.4.2 1
success: change accepted.
```

The following command adds another explicit route, using CIDR notation to specify the subnet mask:

```
DWS-1008# set ip route 192.168.5.0/24 10.5.5.2 1
success: change accepted.
```

# set ip snmp server

Enables or disables the SNMP service on the switch.

**Syntax: set ip snmp server {enable | disable}**

**enable** Enables the SNMP service.

**disable** Disables the SNMP service.

**Defaults:** The SNMP service is disabled by default.

**Access:** Enabled.

**Examples:** The following command enables the SNMP server on a DWS-1008 switch:

```
DWS-1008# set ip snmp server enable
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set ip ssh

Changes the TCP port number on which a DWS-1008 switch listens for Secure Shell (SSH) management traffic.

**Caution:** If you change the SSH port number from an SSH session, MSS immediately ends the session. To open a new management session, you must configure the SSH client to use the new TCP port number.

**Syntax: set ip ssh port** *port-num*

*port-num* TCP port number.

**Defaults:** The default SSH port number is 22.

**Access:** Enabled.

**Examples:** The following command changes the SSH port number on a DWS-1008 switch to 6000:

```
DWS-1008# set ip ssh port 6000
success: change accepted.
```

# set ip ssh server

Disables or reenables the SSH server on a DWS-1008 switch.

**Caution:** If you disable the SSH server, SSH access to the switch is also disabled.

**Syntax: set ip ssh server {enable | disable}**

**enable** Enables the SSH server.

**disable** Disables the SSH server.

**Defaults:** The SSH server is enabled by default.

**Access:** Enabled.

**Usage:** SSH requires an SSH authentication key. You can generate one or allow MSS to generate one. The first time an SSH client attempts to access the SSH server on a DWS-1008 switch, the switch automatically generates a 1024-byte SSH key.

If you want to use a 2048-byte key instead, use the **crypto generate key ssh 2048** command to generate one.

The maximum number of SSH sessions supported on a switch is eight. If Telnet is also enabled, the switch can have up to eight Telnet or SSH sessions, in any combination, and one Console session.


Download from Www.Somanuals.com. All Manuals Search And Download.

# set ip telnet

Changes the TCP port number on which a DWS-1008 switch listens for Telnet management traffic.

**Caution:** If you change the Telnet port number from a Telnet session, MSS immediately ends the session. To open a new management session, you must Telnet to the switch with the new Telnet port number.

**Syntax: set ip telnet** *port-num*

*port-num* TCP port number.

**Defaults:** The default Telnet port number is 23.

**Access:** Enabled.

**Examples:** The following command changes the Telnet port number on a DWS-1008 switch to 5000:

```
DWS-1008# set ip telnet 5000
success: change accepted.
```

**See Also:**
- clear ip telnet
- set ip https server
- set ip telnet server
- show ip https
- show ip telnet

# set ip telnet server

Enables the Telnet server on a DWS-1008 switch.

**Caution:** If you disable the Telnet server, Telnet access to the switch is also disabled.

**Syntax set ip telnet server {enable | disable}**

**enable** Enables the Telnet server.

**disable** Disables the Telnet server.

**Defaults:** The Telnet server is disabled by default.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** The maximum number of Telnet sessions supported on a switch is eight. If SSH is also enabled, the switch can have up to eight Telnet or SSH sessions, in any combination, and one console session.

**Examples:** The following command enables the Telnet server on a DWS-1008 switch:

```
DWS-1008# set ip telnet server enable
success: change accepted.
```

**See Also:**
- clear ip telnet
- set ip https server
- set ip telnet
- show ip https
- show ip telnet

# set ntp

Enables or disables the NTP client on a DWS-1008 switch.

**Syntax: set ntp {enable | disable}**

**enable** Enables the NTP client.

**disable** Disables the NTP client.

**Defaults:** The NTP client is disabled by default.

**Access:** Enabled.

**Usage:** If NTP is configured on a system whose current time differs from the NTP server time by more than 10 minutes, convergence of the switch time can take many NTP update intervals. D-Link recommends that you set the time manually to the NTP server time before enabling NTP to avoid a significant delay in convergence.

**Examples:** The following command enables the NTP client:

```
DWS-1008# set ntp enable
success: NTP Client enabled
```

**See Also:**
- clear ntp server
- clear ntp update-interval
- set ntp server
- set ntp update-interval
- show ntp


Download from Www.Somanuals.com. All Manuals Search And Download.

# set ntp server

Configures a DWS-1008 switch to use an NTP server.

**Syntax: set ntp server** *ip-addr*

*ip-addr* IP address of the NTP server, in dotted decimal notation.

**Defaults:** None.

**Access:** Enabled.

**Usage:** You can configure up to three NTP servers. MSS queries all the servers and selects the best response based on the method described in RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis.

To use NTP, you also must enable the NTP client with the **set ntp** command.

**Examples:** The following command configures a switch to use NTP server 192.168.1.5:

```
DWS-1008# set ntp server 192.168.1.5
```

**See Also:**
- clear ntp server
- clear ntp update-interval
- set ntp
- set ntp update-interval
- show ntp

# set ntp update-interval

Changes how often MSS sends queries to the NTP servers for updates.

**Syntax: set ntp update-interval** *seconds*

*seconds* Number of seconds between queries. You can specify from 16 through 1024 seconds.

**Defaults:** The default NTP update interval is 64 seconds.

**Access:** Enabled.

**Examples:** The following command changes the NTP update interval to 128 seconds:

```
DWS-1008# set ntp update-interval 128
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set snmp community

Configures a community string for SNMPv1 or SNMPv2c.

**Note:** For SNMPv3, use the **set snmp usm** command to configure an SNMPv3 user. SNMPv3 does not use community strings.

**Syntax: set snmp community name** *comm-string*
**access {read-only | read-notify | notify-only | read-write | notify-read-write}**

| | |
|---|---|
| *comm-string* | Name of the SNMP community. Specify between 1 and 32 alphanumeric characters, with no spaces. |
| **read-only** | Allows an SNMP management application using the string to get (read) object values on the switch but not to set (write) them. |
| **read-notify** | Allows an SNMP management application using the string to get object values on the switch but not to set them. The switch can use the string to send notifications. |
| **notify-only** | Allows the switch to use the string to send notifications. |
| **read-write** | Allows an SNMP management application using the string to get and set object values on the switch. |
| **notify-read-write** | Allows an SNMP management application using the string to get and set object values on the switch. The switch also can use the string to send notifications. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** SNMP community strings are passed as clear text in SNMPv1 and SNMPv2c. D-Link recommends that you use strings that cannot easily be guessed by unauthorized users. For example, do not use the well-known strings public and private.

If you are using SNMPv3, you can configure SNMPv3 users to use authentication and to encrypt SNMP data.

**Examples:** The following command configures the read-write community *good_community*:

```
DWS-1008# set snmp community read-write good_community
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The following command configures community string *switchmgr1* with access level notify-read-write:

```
DWS-1008# set snmp community name switchmgr1 notify-read-write
success: change accepted.
```

**See Also:**
- clear snmp community
- set ip snmp server
- set snmp notify target
- set snmp notify profile
- set snmp protocol
- set snmp security
- set snmp usm
- show snmp community

# set snmp notify profile

Configures an SNMP notification profile. A notification profile is a named list of all the notification types that can be generated by a switch, and for each notification type, the action to take (drop or send) when an event occurs.

You can configure up to ten notification profiles.

**Syntax: set snmp notify profile {default |** *profile-name***}**
**{drop | send} {***notification-type* **| all}**

| | |
|---|---|
| **default** \| *profile-name* | Name of the notification profile you are creating or modifying. The profile-name can be up to 32 alphanumeric characters long, with no spaces.<br>To modify the default notification profile, specify **default**. |
| **drop \| send** | Specifies the action that the SNMP engine takes with regard to the notifications you specify with notification-type or all. |
| *notification-type* | Name of the notification type: |

- **APBootTraps**—Generated when an access point boots.
- **ApNonOperStatusTraps**—Generated to indicate an AP radio is nonoperational.
- **ApOperRadioStatusTraps**—Generated when the status of an AP radio changes.
- **APTimeoutTraps**—Generated when an access point fails to respond to the switch.
- **AuthenTraps**—Generated when the switch's SNMP engine receives a bad community string.
- **AutoTuneRadioChannelChangeTraps**—Generated when the RF Auto-Tuning feature changes the channel on a radio.


Download from Www.Somanuals.com. All Manuals Search And Download.

- **AutoTuneRadioPowerChangeTraps**—Generated when the RFAuto-Tuning feature changes the power setting on a radio.
- **ClientAssociationFailureTraps**—Generated when a client's attempt to associate with a radio fails.
- **ClientAuthorizationSuccessTraps**—Generated when a client is successfully authorized.
- **ClientAuthenticationFailureTraps**—Generated when authentication fails for a client.
- **ClientAuthorizationFailureTraps**—Generated when authorization fails for a client.
- **ClientClearedTraps**—Generated when a client's session is cleared.
- **ClientDeAssociationTraps**—Generated when a client is dissociated from a radio.
- **ClientDot1xFailureTraps**—Generated when a client experiences an 802.1X failure.
- **CounterMeasureStartTraps**—Generated when MSS begins countermeasures against a rogue access point.
- **CounterMeasureStopTraps**—Generated when MSS stops countermeasures against a rogue access point.
- **DAPConnectWarningTraps**—Generated when a Distributed MP whose fingerprint has not been configured in MSS establishes a management session with the switch.
- **DeviceFailTraps**—Generated when an event with an Alert severity occurs.
- **DeviceOkayTraps**—Generated when a device returns to its normal state.
- **LinkDownTraps**—Generated when the link is lost on a port.
- **LinkUpTraps**—Generated when the link is detected on a port.
- **MichaelMICFailureTraps**—Generated when two Michael message integrity code (MIC) failures occur within 60 seconds, triggering Wi-Fi Protected Access (WPA) countermeasures.
- **PoEFailTraps**—Generated when a serious PoE problem, such as a short circuit, occurs.
- **RFDetectAdhocUserTraps**—Generated when MSS detects an ad-hoc user.
- **RFDetectRogueAPTraps**—Generated when MSS detects a rogue access point.
- **RFDetectRogueDisappearTraps**—Generated when a rogue access point is no longer being detected.
- **RFDetectClientViaRogueWiredAPTraps**—Generated when MSS detects, on the wired part of the network, the MAC address of a wireless client associated with a third-party AP.
- **RFDetectDoSPortTraps**—Generated when MSS detects an associate request flood, reassociate request flood, or disassociate request flood.
- **RFDetectDoSTraps**—Generated when MSS detects a DoS attack other than an associate request flood, reassociate request flood, or disassociate request flood.
- **RFDetectInterferingRogueAPTraps**—Generated when an interfering device is detected.
- **RFDetectInterferingRogueDisappearTraps**—Generated when an interfering device is no longer detected.


Download from Www.Somanuals.com. All Manuals Search And Download.

- **RFDetectSpoofedMacAPTraps**—Generated when MSS detects a wireless packet with the source MAC address of a D-Link AP, but without the spoofed MP's signature (fingerprint).
- **RFDetectSpoofedSsidAPTraps**—Generated when MSS detects beacon frames for a valid SSID, but sent by a rogue AP.
- **RFDetectUnAuthorizedAPTraps**—Generated when MSS detects the MAC address of an AP that is on the attack list.
- **RFDetectUnAuthorizedOuiTraps**—Generated when a wireless device that is not on the list of permitted vendors is detected.
- **RFDetectUnAuthorizedSsidTraps**—Generated when an SSID that is not on the permitted SSID list is detected.

**all** Sends or drops all notifications.

**Defaults:** A default notification profile (named default) is already configured in MSS. All notifications in the default profile are dropped by default.

**Access:** Enabled.

**Examples:** The following command changes the action in the default notification profile from drop to send for all notification types:

```
DWS-1008# set snmp notify profile default send all
success: change accepted.
```

The following commands create notification profile *snmpprof_rfdetect*, and change the action to send for all RF detection notification types:

```
DWS-1008# set snmp notify profile snmpprof_rfdetect send
RFDetectAdhocUserTraps
success: change accepted.

DWS-1008# set snmp notify profile snmpprof_rfdetect send
RFDetectClientViaRogueWiredAPTraps
success: change accepted.

DWS-1008# set snmp notify profile snmpprof_rfdetect send RFDetectDoSTraps
success: change accepted.

DWS-1008# set snmp notify profile snmpprof_rfdetect send
RFDetectAdhocUserTraps
success: change accepted.

DWS-1008# set snmp notify profile snmpprof_rfdetect send
RFDetectInterferingRogueAPTraps
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

DWS-1008# **set snmp notify profile snmpprof_rfdetect send RFDetectInterferingRogueDisappearTraps**
success: change accepted.

DWS-1008# **set snmp notify profile snmpprof_rfdetect send RFDetectRogueAPTraps**
success: change accepted.

DWS-1008# **set snmp notify profile snmpprof_rfdetect send RFDetectRogueDisappearTraps**
success: change accepted.

DWS-1008# **set snmp notify profile snmpprof_rfdetect send RFDetectSpoofedMacAPTraps**
success: change accepted.

DWS-1008# **set snmp notify profile snmpprof_rfdetect send RFDetectSpoofedSsidAPTraps**
success: change accepted.

DWS-1008# **set snmp notify profile snmpprof_rfdetect send RFDetectUnAuthorizedAPTraps**
success: change accepted.

DWS-1008# **set snmp notify profile snmpprof_rfdetect send RFDetectUnAuthorizedOuiTraps**
success: change accepted.

DWS-1008# **set snmp notify profile snmpprof_rfdetect send RFDetectUnAuthorizedSsidTraps**
success: change accepted.

**See Also:**
- clear snmp notify profile
- set ip snmp server
- set snmp community
- set snmp notify target
- set snmp protocol
- set snmp security
- set snmp usm
- show snmp notify profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set snmp notify target

Configures a notification target for notifications from SNMP.

A notification target is a remote device to which MSS sends SNMP notifications. You can configure the MSS SNMP engine to send confirmed notifications (informs) or unconfirmed notifications (traps). Some of the command options differ depending on the SNMP version and the type of notification you specify.

You can configure up to 10 notification targets.

**SNMPv3 with Informs**

To configure a notification target for informs from SNMPv3, use the following command:

**Syntax: set snmp notify target** *target-num ip-addr* **[***:udp-port-number***]**
**usm inform user** *username* **snmp-engine-id {ip | hex** *hex-string***}**
**[profile** *profile-name***] [security {unsecured | authenticated | encrypted}]**
**[retries** *num***] [timeout** *num***]**

| | |
|---|---|
| *target-num* | ID for the target. This ID is local to the switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10. |
| *ip-addr[:udp-port-number]* | IP address of the server. You also can specify the UDP port number to send notifications to. |
| *username* | USM username. This option is applicable only when the SNMP version is usm. If the user will send informs rather than traps, you also must specify the snmp-engine-id of the target. |
| **snmp-engine-id {ip \| hex** *hex-string***}** | SNMP engine ID of the target. Specify ip if SNMP engine ID the target's SNMP engine ID is based on its IP address. If the target's SNMP engine ID is a hexadecimal value, use hex hex-string to specify the value. |
| **profile** *profile-name* | Notification profile this SNMP user will use to specify the notification types to send or drop. |
| **security {unsecured \| authenticated \| encrypted}** | Specifies the security level, and is applicable only when the SNMP version is usm:<br>• **unsecured**—Message exchanges are not authenticated, nor are they encrypted. This is the default.<br>• **authenticated**—Message exchanges are authenticated, but are not encrypted.<br>• **encrypted**—Message exchanges are authenticated and encrypted. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| **retries** *num* | Specifies the number of times the MSS SNMP engine will resend a notification that has not been acknowledged by the target. You can specify from 0 to 3 retries. |
| **timeout** *num* | Specifies the number of seconds MSS waits for acknowledgement of a notification. You can specify from 1 to 5 seconds. |

**SNMPv3 with Traps**

To configure a notification target for traps from SNMPv3, use the following command:

**Syntax: set snmp notify target** *target-num ip-addr* **[***:udp-port-number***]**
**usm trap user** *username* **[profile** *profile-name***] [security {unsecured | authenticated | encrypted}]**

| | |
|---|---|
| *target-num* | ID for the target. This ID is local to the switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10. |
| *ip-addr[:udp-port-number]* | IP address of the server. You also can specify the UDP port number to send notifications to. |
| *username* | USM username. This option is applicable only when the SNMP version is usm. |
| **profile** *profile-name* | Notification profile this SNMP user will use to specify the notification types to send or drop. |
| **security {unsecured \| authenticated \| encrypted}** | Specifies the security level, and is applicable only when the SNMP version is usm:<br>• **unsecured**—Message exchanges are not authenticated, nor are they encrypted. This is the default.<br>• **authenticated**—Message exchanges are authenticated, but are not encrypted.<br>• **encrypted**—Message exchanges are authenticated and encrypted. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**SNMPv2c with Informs**

To configure a notification target for informs from SNMPv2c, use the following command:

**Syntax: set snmp notify target** *target-num ip-addr* **[***:udp-port-number***]**
**v2c** *community-string* **inform [profile** *profile-name***] [retries** *num***] [timeout** *num***]**

| | |
|---|---|
| *target-num* | ID for the target. This ID is local to the switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10. |
| *ip-addr [:udp-port-number]* | IP address of the server. You also can specify the UDP port number to send notifications to. |
| *community-string* | Community string. |
| **profile** *profile-name* | Notification profile this SNMP user will use to specify the notification types to send or drop. |
| **retries** *num* | Specifies the number of times the MSS SNMP engine will resend a notification that has not been acknowledged by the target. You can specify from 0 to 3 retries. |
| **timeout** *num* | Specifies the number of seconds MSS waits for acknowledgement of a notification. You can specify from 1 to 5 seconds. |

**SNMPv2c with Traps**

To configure a notification target for traps from SNMPv2c, use the following command:

**Syntax: set snmp notify target** *target-num ip-addr* **[***:udp-port-number***]**
**v2c** *community-string* **trap [profile** *profile-name***]**

| | |
|---|---|
| *target-num* | ID for the target. This ID is local to the switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10. |
| *ip-addr [:udp-port-number]* | IP address of the server. You also can specify the UDP port number to send notifications to. |
| *community-string* | Community string. |
| **profile** *profile-name* | Notification profile this SNMP user will use to specify the notification types to send or drop. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**SNMPv1 with Traps**

To configure a notification target for traps from SNMPv1, use the following command:

**Syntax: set snmp notify target** *target-num ip-addr* **[***:udp-port-number***]**
**v1** *community-string* **[profile** *profile-name***]**

| | |
|---|---|
| *target-num* | ID for the target. This ID is local to the switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10. |
| *ip-addr [:udp-port-number]* | IP address of the server. You also can specify the UDP port number to send notifications to. |
| *community-string* | Community string. |
| **profile** *profile-name* | Notification profile this SNMP user will use to specify the notification types to send or drop. |

**Defaults:** The default UDP port number on the target is 162. The default minimum required security level is unsecured. The default number of retries is 0 and the default timeout is 2 seconds.

**Access:** Enabled.

**Usage:** The inform or trap option specifies whether the MSS SNMP engine expects the target to acknowledge notifications sent to the target by the switch. Use inform if you want acknowledgements. Use trap if you do not want acknowledgements. The inform option is applicable to SNMP version v2c or usm only.

**Examples:** The following command configures a notification target for acknowledged notifications:

```
DWS-1008# set snmp notify target 1 10.10.40.9 usm inform user securesnmpmgr1
snmp-engine-id ip
success: change accepted.
```

This command configures target 1 at IP address 10.10.40.9. The target's SNMP engine ID is based on its address. The MSS SNMP engine will send notifications based on the default profile, and will require the target to acknowledge receiving them.

The following command configures a notification target for unacknowledged notifications:

```
DWS-1008# set snmp notify target 2 10.10.40.10 v1 trap
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set snmp protocol

Enables an SNMP protocol. MSS supports SNMPv1, SNMPv2c, and SNMPv3.

**Syntax: set snmp protocol {v1 | v2c | usm | all} {enable | disable}**

| | |
|---|---|
| **v1** | SNMPv1 |
| **v2c** | SNMPv2c |
| **usm** | SNMPv3 (with the user security model) |
| **all** | Enables all supported versions of SNMP. |
| **enable** | Enables the specified SNMP version(s). |
| **disable** | Disables the specified SNMP version(s). |

**Defaults:** All SNMP versions are disabled by default.

**Access:** Enabled.

**Usage:** SNMP requires the switch's system IP address to be set. SNMP will not work without the system IP address. You also must enable the SNMP service using the set ip snmp server command.

**Examples:** The following command enables all SNMP versions:

```
DWS-1008# set snmp protocol all enable
success: change accepted.
```

**See Also:**
- set ip snmp server
- set snmp community
- set snmp notify target
- set snmp notify profile
- set snmp security
- set snmp usm
- show snmp status

# set snmp security

Sets the minimum level of security MSS requires for SNMP message exchanges.

**Syntax: set snmp security {unsecured | authenticated | encrypted | auth-req-unsec-notify}**

| | |
|---|---|
| **unsecured** | SNMP message exchanges are not secure. This is the only value supported for SNMPv1 and SNMPv2c. |
| **authenticated** | SNMP message exchanges are authenticated but are not encrypted. |
| **encrypted** | SNMP message exchanges are authenticated and encrypted. |
| **auth-req-unsecnotify** | SNMP message exchanges are authenticated but are not encrypted, and notifications are neither authenticated nor encrypted. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** By default, MSS allows nonsecure (unsecured) SNMP message exchanges.

**Access:** Enabled.

**Usage:** SNMPv1 and SNMPv2c do not support authentication or encryption. If you plan to use SNMPv1 or SNMPv2c, leave the minimum level of SNMP security set to unsecured.

**Examples:** The following command sets the minimum level of SNMP security allowed to authentication and encryption:

```
DWS-1008# set snmp security encrypted
success: change accepted.
```

**See Also:**
- set ip snmp server
- set snmp community
- set snmp notify target
- set snmp notify profile
- set snmp protocol
- set snmp usm
- show snmp status

# set snmp usm

Creates a USM user for SNMPv3.

**Note:** This command does not apply to SNMPv1 or SNMPv2c. For these SNMP versions, use the **set snmp community** command to configure community strings.

**Syntax: set snmp usm** *usm-username* **snmp-engine-id {ip** *ip-addr* **| local | hex** *hex-string***}**
**access {read-only | read-notify | notify-only | read-write | notify-read-write}**
**auth-type {none | md5 | sha} {auth-pass-phrase** *string* **| auth-key** *hex-string***}**
**encrypt-type {none | des | 3des | aes} {encrypt-pass-phrase** *string* **|**
**encrypt-key** *hex-string***}**

| | |
|---|---|
| *usm-username* | Name of the SNMPv3 user. Specify between 1 and 32 alphanumeric characters, with no spaces. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| **snmp-engine-id {ip** *ip-addr* **\| local \| hex** *hex-string***}** | Specifies a unique identifier for the SNMP engine. To send informs, you must specify the engine ID of the inform receiver.<br><br>To send traps and to allow get and set operations and so on, specify local as the engine ID.<br><br>• **hex** *hex-string*—ID is a hexadecimal string.<br><br>• **ip** *ip-addr*—ID is based on the IP address of the station running the management application. Enter the IP address of the station. MSS calculates the engine ID based on the address.<br><br>• **local**—Uses the value computed from the switch's system IP address. |
| **access {read-only \| read-notify \| notify-only \| read-write \| notify-read-write}** | Specifies the access level of the user:<br><br>• **read-only**—An SNMP management application using the string can get (read) object values on the switch but cannot set (write) them.<br><br>• **read-notify**—An SNMP management application using the string can get object values on the switch but cannot set them. The switch can use the string to send notifications.<br><br>• **notify-only**—The switch can use the string to send notifications.<br><br>• **read-write**—An SNMP management application using the string can get and set object values on the switch.<br><br>• **notify-read-write**—An SNMP management application using the string can get and set object values on the switch. The switch can use the string to send notifications. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| **auth-type {none \| md5 \| sha} {auth-pass-phrase** *string* **\| auth-key** *hex-string***}** | Specifies the authentication type used to authenticate communications with the remote SNMP engine. You can specify one of the following:<br><br>• **none**—No authentication is used.<br>• **md5**—Message-digest algorithm 5 is used.<br>• **sha**—Secure Hashing Algorithm (SHA) is used.<br><br>If the authentication type is **md5** or **sha**, you can specify a passphrase or a hexadecimal key.<br><br>• To specify a passphrase, use the auth-pass-phrase string option. The string can be from 8 to 32 alphanumeric characters long, with no spaces.<br><br>• To specify a key, use the **auth-key** *hex-string* option. |
| **encrypt-type {none \| des \| 3des \|aes} {encrypt-pass-phrase string \| encrypt-key hex-string}** | Specifies the encryption type used for SNMP traffic. You can specify for SNMP traffic. You can specify one of the following:<br><br>• **none**—No encryption is used. This is the default.<br><br>• **des**—Data Encryption Standard (DES) encryption is used.<br><br>• **3des**—Triple DES encryption is used.<br><br>• **aes**—Advanced Encryption Standard (AES) encryption is used.<br><br>If the encryption type is **des**, **3des**, or **aes**, you can specify a passphrase or a hexadecimal key.<br><br>• To specify a passphrase, use the **encrypt-pass-phrase** *string* option. The string can be from 8 to 32 alphanumeric characters long, with no spaces.<br><br>• To specify a key, use the **encrypt-key** *hex-string* option. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** No SNMPv3 users are configured by default. When you configure an SNMPv3 user, the default access is read-only, and the default authentication and encryption types are both none.

**Access:** Enabled.

**Examples:** The following command creates USM user *snmpmgr1*, associated with the local SNMP engine ID. This user can send traps to notification receivers.

```
DWS-1008# set snmp usm snmpmgr1 snmp-engine-id local
success: change accepted.
```

The following command creates USM user *securesnmpmgr1*, which uses SHA authentication and 3DES encryption with passphrases. This user can send informs to the notification receiver that has engine ID 192.168.40.2.

```
DWS-1008# set snmp usm securesnmpmgr1 snmp-engine-id ip 192.168.40.2
auth-type sha auth-pass-phrase myauthpword encrypt-type 3des
encrypt-pass-phrase mycryptpword
success: change accepted.
```

**See Also:**
- clear snmp usm
- set ip snmp server
- set snmp community
- set snmp notify target
- set snmp notify profile
- set snmp protocol
- set snmp security
- show snmp usm

# set summertime

Offsets the real-time clock of a switch by +1 hour and returns it to standard time for daylight savings time or a similar summertime period that you set.

**Syntax: set summertime** *summer-name* **[start** *week weekday month hour min*
**end** *week weekday month hour min***]**

| | |
|---|---|
| *summer-name* | Name of up to 32 alphanumeric characters that describes the summertime offset. You can use a standard name or any name you like. |
| **start** | Start of the time change period. |
| *week* | Week of the month to start or end the time change. Valid values are first, second, third, fourth, or last. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| *weekday* | Day of the week to start or end the time change. Valid values are sun, mon, tue, wed, thu, fri, and sat. |
| *month* | Month of the year to start or end the time change. Valid values are jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, and dec. |
| *hour* | Hour to start or end the time change—a value between 0 and 23 on the 24-hour clock. |
| *min* | Minute to start or end the time change—a value between 0 and 59. |
| **end** | End of the time change period. |

**Defaults:** If you do not specify a **start** and **end** time, the system implements the time change starting at 2:00 a.m. on the first Sunday in April and ending at 2:00 a.m. on the last Sunday in October, according to the North American standard.

**Access:** Enabled.

**Usage:** You must first set the time zone with the **set timezone** command for the offset to work properly without the start and end values. Configure summertime before you set the time and date. Otherwise, summertime's adjustment of the time will make the time incorrect, if the date is within the summertime period.

**Examples:** To enable summertime and set the summertime time zone to PDT (Pacific Daylight Time), type the following command:

```
DWS-1008# set summertime PDT
success: change accepted
```

**See Also:**
- clear summertime
- clear timezone
- set timedate
- set timezone
- show summertime
- show timedate
- show timezone


Download from Www.Somanuals.com. All Manuals Search And Download.

# set system ip-address

Configures the system IP address. The system IP address determines the interface or source IP address MSS uses for system tasks, including the following:

- Topology reporting for dual-homed access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

**Syntax: set system ip-address** *ip-addr*

| | |
|---|---|
| *ip-addr* | IP address, in dotted decimal notation. The address must be configured on one of the DWS-1008 switch's VLANs. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** You must use an address that is configured on one of the switch's VLANs.

To display the system IP address, use the **show system** command.

**Examples:** The following commands configure an IP interface on VLAN *taupe* and configure the interface to be the system IP address:

```
DWS-1008# set interface taupe ip 10.10.20.20/24
success: set ip address 10.10.20.20 netmask 255.255.255.0 on vlan taupe

DWS-1008# set system ip-address 10.10.20.20
success: change accepted.
```

**See Also:**
- clear system ip-address
- set interface
- show system


Download from Www.Somanuals.com. All Manuals Search And Download.

# set timedate

Sets the time of day and date on the switch.

**Syntax: set timedate {date** *mmm dd yyyy* **[time** *hh:mm:ss***]}**

| | |
|---|---|
| **date** *mmm dd yyyy* | System date:<br>• *mmm*—month.<br>• *dd*—day.<br>• *yyyy*—year. |
| **time** *hh:mm:ss* | System time, in hours, minutes, and seconds. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** The day of week is automatically calculated from the day you set. The time displayed by the CLI after you type the command might be slightly later than the time you enter due to the interval between when you press Enter and when the CLI reads and displays the new time and date.

Configure summertime before you set the time and date. Otherwise, summertime's adjustment of the time will make the time incorrect, if the date is within the summertime period.

**Examples:** The following command sets the date to March 13, 2003 and time to 11:11:12:

```
DWS-1008# set timedate date feb 29 2004 time 23:58:00
Time now is: Sun Feb 29 2004, 23:58:02 PST
```

**See Also:**
- clear summertime
- clear timezone
- set summertime
- set timezone
- show summertime
- show timedate
- show timezone

# set timezone

Sets the number of hours, and optionally the number of minutes, that the switch's real-time clock is offset from Coordinated Universal Time (UTC). These values are also used by Network Time Protocol (NTP), if it is enabled.

**Syntax: set timezone** *zone-name* **{**-*hours* **[**-*minutes***]}**


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| *zone-name* | Time zone name of up to 32 alphabetic characters. You can use a standard name or any name you like. |
| - | Minus time to indicate hours (and minutes) to be subtracted from UTC. Otherwise, hours and minutes are added by default. |
| *hours* | Number of hours to add or subtract from UTC. |
| *minutes* | Number of minutes to add or subtract from UTC. |

**Defaults:** If this command is not used, then the default time zone is UTC.

**Access:** Enabled.

**Examples:** To set the time zone for Pacific Standard Time (PST), type the following command:

```
DWS-1008# set timezone PST -8
Timezone is set to 'PST', offset from UTC is -8:0 hours.
```

**See Also:**
- clear summertime
- clear timezone
- set summertime
- set timedate
- show summertime
- show timedate
- show timezone

# show arp

Displays the ARP table.

**Syntax: show arp [***ip-addr***]**

| | |
|---|---|
| *ip-addr* | IP address. |

**Defaults:** If you do not specify an IP address, the whole ARP table is displayed.

**Access:** All.

**Examples:** The following command displays ARP entries:

```
DWS-1008# show arp
ARP aging time: 1200 seconds
Host          HW Address         VLAN  Type          State
--------------------------------------------------------------------------------
10.5.4.51     00:0b:0e:02:76:f5  1     DYNAMIC       RESOLVED
10.5.4.53     00:0b:0e:02:76:f7  1     LOCAL         RESOLVED
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields in this display.

| Field | Description |
|---|---|
| ARP aging time | Number of seconds a dynamic entry can remain unused before MSS removes the entry from the ARP table. |
| Host | IP address, hostname, or alias. |
| HW Address | MAC address mapped to the IP address, hostname, or alias. |
| VLAN | VLAN the entry is for. |
| Type | Entry type:<br>• **DYNAMIC**—Entry was learned from network traffic and ages out if unused for longer than the ARP aging timeout.<br>• **LOCAL**—Entry for the switch MAC address. Each VLAN has one local entry for the switch MAC address.<br>• **PERMANENT**—Entry does not age out and remains in the configuration even following a reboot.<br>• **STATIC**—Entry does not age out but is removed after a reboot. |
| State | Entry state:<br>• **RESOLVING**—MSS sent an ARP request for the entry and is waiting for the reply.<br>• **RESOLVED**—Entry is resolved. |

**See Also:**
• set arp
• set arp agingtime

# show dhcp-client

Displays DHCP client information for all VLANs.

**Syntax:** show dhcp-client

**Defaults:** None.

**Access:** All.

**Examples:** The following command displays DHCP client information:

```
DWS-1008# show dhcp-client
Interface:              corpvlan(4)
Configuration Status:   Enabled
DHCP State:             IF_UP
Lease Allocation:       65535 seconds
Lease Remaining:        65532 seconds
IP Address:             10.3.1.110
Subnet Mask:            255.255.255.0
Default Gateway:        10.3.1.1
DHCP Server:            10.3.1.4
DNS Servers:            10.3.1.29
DNS Domain Name:        mycorp.com
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Interface | VLAN name and number. |
| Configuration Status | Status of the DHCP client on this VLAN:<br>• Enabled<br>• Disabled |
| DHCP State | State of the IP interface:<br>• IF_UP<br>• IF_DOWN |
| Lease Allocation | Duration of the address lease. |
| Lease Remaining | Number of seconds remaining before the address lease expires. |
| IP Address | IP address received from the DHCP server. |
| Subnet Mask | Network mask of the IP address received from the DHCP server. |
| Default Gateway | Default router (gateway) IP address received from the DHCP server. If the address is 0.0.0.0, the server did not provide an address. |
| DHCP Server | IP address of the DHCP server. |
| DNS Servers | DNS server IP address(es) received from the DHCP server. |
| DNS Domain Name | Default DNS domain name received from the DHCP server. |

**See Also:**
• set interface dhcp-client

# show dhcp-server

Displays MSS DHCP server information.

**Syntax: show dhcp-server [interface** *vlan-id***] [verbose]**

**interface** *vlan-id* Displays the IP addresses leased by the specified VLAN.

**verbose** Displays configuration and status information for the MSS DHCP server.

**Defaults:** None.

**Access:** All.

**Examples:** The following command displays the addresses leased by the MSS DHCP server:

```
DWS-1008# show dhcp-server
VLAN  Name        Address     MAC                Lease Remaining (sec)
-------------------------------------------------------------------------------
1     default     10.10.20.2  00:01:02:03:04:05        12345
1     default     10.10.20.3  00:01:03:04:06:07        2103
2     red-vlan    192.168.1.5 00:01:03:04:06:08        102
2     red-vlan    192.168.1.7 00:01:03:04:06:09        16789
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The following command displays configuration and status information for each VLAN on which the DHCP server is configured:

```
DWS-1008# show dhcp-server verbose
Interface:          0 (Direct AP)
Status:             UP
Address Range:      10.0.0.1-10.0.0.253
Interface:          default(1)
Status:             UP
Address Range:      10.10.20.2-10.10.20.254
Hardware Address:   00:01:02:03:04:05
State:              BOUND
Lease Allocation:   43200 seconds
Lease Remaining:    12345 seconds
IP Address:         10.10.20.2
Subnet Mask:        255.255.255.0
Default Router:     10.10.20.1
DNS Servers:        10.10.20.4 10.10.20.5
DNS Domain Name: mycorp.com
```

The table below shows the output for **show dhcp-server:**

| Field | Description |
|---|---|
| VLAN | VLAN number. |
| Name | VLAN name. |
| Address | IP address leased by the server. |
| MAC Address | MAC address of the device that holds the lease for the address. |
| Lease Remaining | Number of seconds remaining before the address lease expires. |

The table below shows the output for **show dhcp-server verbose:**

| Field | Description |
|---|---|
| Interface | VLAN name and number. |
| Status | Status of the interface:<br>• UP<br>• DOWN |
| Address Range | Range from which the server can lease addresses. |
| Hardware Address | MAC address of the DHCP client. |
| State | State of the address lease:<br>• **SUSPEND**—MSS is checking for the presence of another DHCP server on the subnet. This is the initial state of the MSS DHCP server. The MSS DHCP server remains in this state if another DHCP server is detected.<br>• **CHECKING**—MSS is using ARP to verify whether the address is available.<br>• **OFFERING**—MSS offered the address to the client and is waiting for the client to send a DHCPREQUEST for the address.<br>• **BOUND**—The client accepted the address.<br>• **HOLDING**—The address is already in use and is therefore unavailable. |
| Lease Allocation | Duration of the address lease, in seconds. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| Lease Remaining | Number of seconds remaining before the address lease expires. |
| IP Address | IP address leased to the client. |
| Subnet Mask | Network mask of the IP address leased to the client. |
| Default Router | Default router IP address included in the DHCP Offer to the client. |
| DNS Servers | DNS server IP address(es) included in the DHCP Offer to the client. |
| DNS Domain Name | Default DNS domain name included in the DHCP Offer to the client. |

# show interface

Displays the IP interfaces configured on the switch.

**Syntax: show interface [*vlan-id*]**

*vlan-id* VLAN name or number.

**Defaults:** If you do not specify a VLAN ID, interfaces for all VLANs are displayed.

**Access:** All

**Usage:** The IP interface table flags an address assigned by a DHCP server with an asterisk (*).

**Examples:** The following command displays all the IP interfaces configured on a switch:

```
DWS-1008# show interface
VLAN  Name      Address     Mask            Enabled   State  RIB
-------------------------------------------------------------------------------
1     default   10.10.10.10 255.255.255.0   YES       Up     ipv4
2     mauve     10.10.20.10 255.255.255.0   NO        Down   ipv4
4     corpvlan  *10.3.1.110 255.255.255.0   YES       Up     ipv4
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| VLAN | VLAN number. |
| Name | VLAN name. |
| Address | IP address. |
| Mask | Subnet mask. |
| Enabled | Administrative state:<br>• YES (enabled)<br>• NO (disabled) |
| State | Link state:<br>• Up (operational)<br>• Down (unavailable) |
| RIB | Routing Information Base |


Download from Www.Somanuals.com. All Manuals Search And Download.

# show ip alias

Displays the IP aliases configured on the DWS-1008 switch.

**Syntax: show ip alias [***name***]**

*name* Alias string.

**Defaults:** If you do not specify an alias name, all aliases are displayed.

**Access:** Enabled.

**Examples:** The following command displays all the aliases configured on a switch:

```
DWS-1008# show ip alias
Name          IP Address
--------------------------------
HR1           192.168.1.2
payroll       192.168.1.3
radius1       192.168.7.2
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Name | Alias string. |
| IP Address | IP address associated with the alias. |

**See Also:**
- clear ip alias
- set ip alias


Download from Www.Somanuals.com. All Manuals Search And Download.

# show ip dns

Displays the DNS servers the switch is configured to use.

**Syntax: show ip dns**

**Defaults:** None.

**Access:** All.

**Examples:** The following command displays the DNS information:

```
DWS-1008# show ip dns
Domain Name: example.com
DNS Status: enabled
IP Address    Type
-------------------------------------
10.1.1.1      PRIMARY
10.1.1.2      SECONDARY
10.1.2.1      SECONDARY
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Domain Name | Default domain name configured on the switch |
| DNS Status | Status of the switch's DNS client:<br>• Enabled<br>• Disabled |
| IP Address | IP address of the DNS server |
| Type | Server type:<br>• PRIMARY<br>• SECONDARY |

**See Also:**
- clear ip dns domain
- clear ip dns server
- set ip dns
- set ip dns domain
- set ip dns server


Download from Www.Somanuals.com. All Manuals Search And Download.

# show ip https

Displays information about the HTTPS management port.

**Syntax: show ip https**

**Defaults:** None.

**Access:** All.

**Examples:** The following command shows the status and port number for the HTTPS management interface to the switch:

```
DWS-1008> show ip https
HTTPS is enabled
HTTPS is set to use port 443
Last 10 Connections:
IP Address     Last Connected      Time Ago (s)
-------------------------------------------------------------------------------
10.10.10.56    2003/05/09          15:51:26 pst 349
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| HTTPS is enabled/disabled | State of the HTTPS server:<br>• Enabled<br>• Disabled |
| HTTPS is set to use port | TCP port number on which the switch listens for HTTPS connections. |
| Last 10 connections | List of the last 10 devices to establish connections to the switch's HTTPS server. |
| IP Address | IP address of the device that established the connection.<br><br>**Note:** If a browser connects to a switch from behind a proxy, then only the proxy IP address is shown. If multiple browsers connect using the same proxy, the proxy address appears only once in the output. |
| Last Connected | Time when the device established the HTTPS connection to the switch. |
| Time Ago (s) | Number of seconds since the device established the HTTPS connection to the switch. |

**See Also:**
- clear ip telnet
- set ip https server
- set ip telnet
- set ip telnet server
- show ip telnet


Download from Www.Somanuals.com. All Manuals Search And Download.

# show ip route

Displays the IP route table.

**Syntax: show ip route [*destination*]**

*destination* Route destination IP address, in dotted decimal notation.

**Defaults:** None.

**Access:** All.

**Usage:** When you add an IP interface to a VLAN that is up, MSS adds direct and local routes for the interface to the route table. If the VLAN is down, MSS does not add the routes. If you add an interface to a VLAN but the routes for that interface do not appear in the route table, use the show vlan config command to check the VLAN state.

If you add a static route and the route's state is shown as Down, use the show interface command to verify that the has an IP interface in the default router's (gateway's) subnet. MSS cannot resolve a static route unless one of the switch's VLANs has an interface in the default router's subnet. If the switch has such an interface but the static route is still down, use the show vlan config command to check the state of the VLAN's ports.

**Examples:** The following command shows all routes in a switch's IP route table:

```
DWS-1008# show ip route
Router table for IPv4
Destination/Mask    Proto  Metric    NH-Type    Gateway    VLAN:Interface
-------------------------------------------------------------------------
0.0.0.0/ 0          Static 1         Router     10.0.1.17  Down
0.0.0.0/ 0          Static 2         Router     10.0.2.17  vlan:2:ip
10.0.2.1/24         IP     0         Direct                vlan:2:ip
10.0.2.1/32         IP     0         Direct                vlan:2:ip:10.0.1.1/24
10.0.2.255/32       IP     0         Direct                vlan:2:ip:10.0.1.1/24
224.0.0.0/ 4        IP     0         Local                 MULTICAST
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Destination/Mask | IP address and subnet mask of the route destination. The 244.0.0.0 route is automatically added by MSS and supports the IGMP snooping feature. |
| Proto | Protocol that added the route to the IP route table. The protocol can be one of the following:<br>• IP—MSS added the route.<br>• Static—An administrator added the route. |
| Metric | Cost for using the route. |
| NH-Type | Next-hop type:<br>• Local—Route is for a local interface. MSS adds the route when you configure an IP address on the switch.<br>• Direct—Route is for a locally attached subnet. MSS adds the route when you add an interface in the same subnet to the switch.<br>• Router—Route is for a remote destination. A switch forwards traffic for the destination to the default router (gateway). |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| Gateway | Next-hop router for reaching the route destination.<br>**Note:** This field applies only to static routes. |
| VLAN:Interface | Destination VLAN, protocol type, and IP address of the route. Because direct routes are for local interfaces, a destination IP address is not listed. The destination for the IP multicast route is MULTICAST.<br>For static routes, the value Down means the switch does not have an interface to the destination's next-hop router. To provide an interface, configure an IP interface that is in the same IP subnet as the next-hop router. The IP interface must be on a VLAN containing the port that is attached to the default router. |

# show ip telnet

Displays information about the Telnet management port.

**Syntax: show ip telnet**

**Defaults:** None.

**Access:** All.

**Examples:** The following command shows the status and port number for the Telnet management interface to the switch:

```
DWS-1008> show ip telnet
Server Status        Port
---------------------------------
Enabled              23
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Server Status | State of the HTTPS server:<br>• Enabled<br>• Disabled |
| Port | TCP port number on which the switch listens for Telnet management traffic. |

**See Also:**
- clear ip telnet
- set ip https server
- set ip telnet
- set ip telnet server
- show ip https


Download from Www.Somanuals.com. All Manuals Search And Download.

# show ntp

Displays NTP client information.

**Syntax: show ntp**

**Defaults:** None.

**Access:** All.

**Examples:** To display NTP information for a DWS-1008 switch, type the following command:

```
DWS-1008> show ntp
NTP client: enabled
Current update-interval: 20(secs)
Current time: Fri Feb 06 2004, 12:02:57
Timezone is set to 'PST', offset from UTC is -8:0 hours.
Summertime is enabled.
Last NTP update: Fri Feb 06 2004, 12:02:46
NTP Server          Peer state          Local State
---------------------------------------------------------------------
192.168.1.5         SYSPEER             SYNCED
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| NTP client | State of the NTP client. The state can be one of the following:<br>• Enabled<br>• Disabled |
| Current update-interval | Number of seconds between queries sent by the switch to the NTP servers for updates. |
| Current time | System time that was current on the switch when you pressed Enter after typing the **show ntp** command. |
| Timezone | Time zone configured on the switch. MSS offsets the time reported by the NTP server based on the time zone.<br>**Note:** This field is displayed only if you change the time zone. |
| Summertime | Summertime period configured on the switch. MSS offsets the system time +1 hour and returns it to standard time for daylight savings time or a similar summertime period that you set.<br>**Note:** This field is displayed only if you enable summertime. |
| Last NTP update | Time when the switch received the most recent update from an NTP server. |
| NTP Server | IP address of the NTP server. |
| Peer state | State of the NTP session from the point of view of the NTP server:<br>• CORRECT<br>• REJECT<br>• SELCAND<br>• SYNCCAND<br>• SYSPEER |
| Local state | State of the NTP session from the point of view of the switch's NTP client:<br>• INITED<br>• START<br>• SYNCED |


Download from Www.Somanuals.com. All Manuals Search And Download.

## show snmp community

Displays the configured SNMP community strings.

**Syntax: show snmp community**

**Defaults:** None.

**Access:** Enabled.

**See Also:**
- clear snmp community
- set snmp community

## show snmp counters

Displays SNMP statistics counters.

**Syntax: show snmp counters**

**Defaults:** None.

**Access:** Enabled.

## show snmp notify profile

Displays SNMP notification profiles.

**Syntax: show snmp notify profile**

**Defaults:** None.

**Access:** Enabled.

**See Also:**
- clear snmp notify profile
- set snmp notify profile

## show snmp notify target

Displays SNMP notification targets.

**Syntax: show snmp notify target**

**Defaults:** None.

**Access:** Enabled.

**See Also:**
- clear snmp notify target
- set snmp notify target


Download from Www.Somanuals.com. All Manuals Search And Download.

# show snmp status

Displays SNMP version and status information.

**Syntax: show snmp status**

**Defaults:** None.

**Access:** Enabled.

**See Also:**
- set snmp community
- set snmp notify target
- set snmp notify profile
- set snmp protocol
- set snmp security
- set snmp usm
- show snmp community
- show snmp counters
- show snmp notify profile
- show snmp notify target
- show snmp usm

# show snmp usm

Displays information about SNMPv3 users.

**Defaults:** None.

**Access:** Enabled.

**See Also:**
- clear snmp usm
- show snmp usm


Download from Www.Somanuals.com. All Manuals Search And Download.

# show summertime

Shows a switch's offset from its real-time clock.

**Syntax: show summertime**

**Defaults:** There is no summertime offset by default.

**Access:** All.

**Examples:** To display the summertime setting on a switch, type the following command:

```
DWS-1008# show summertime
Summertime is enabled, and set to 'PDT'.
Start : Sun Apr 04 2004, 02:00:00
End : Sun Oct 31 2004, 02:00:00
Offset : 60 minutes
Recurring : yes, starting at 2:00 am of first Sunday of April
and ending at 2:00 am on last Sunday of October.
```

**See Also:**
- clear summertime
- clear timezone
- set summertime
- set timedate
- set timezone
- show timedate
- show timezone

# show timedate

Shows the date and time of day currently set on a DWS-1008 switch's real-time clock.

**Syntax: show timedate**

**Defaults:** None.

**Access:** All.

**Examples:** To display the time and date set on a switch's real-time clock, type the following command:

```
DWS-1008# show timedate
Sun Feb 29 2004, 23:59:02 PST
```

**See Also:**
- clear summertime
- clear timezone
- set summertime
- set timedate
- set timezone
- show summertime
- show timezone


Download from Www.Somanuals.com. All Manuals Search And Download.

# show timezone

Shows the time offset for the real-time clock from UTC on a switch.

**Syntax: show timezone**

**Defaults:** None.

**Access:** All.

**Examples:** To display the offset from UTC, type the following command:

```
DWS-1008# show timezone
Timezone set to 'pst', offset from UTC is -8 hours
```

**See Also:**
- clear summertime
- clear timezone
- set summertime
- set timedate
- set timezone
- show summertime
- show timedate

# telnet

Opens a Telnet client session with a remote device.

**Syntax: telnet {***ip-addr* **|** *hostname***} [port** *port-num***]**

| | |
|---|---|
| *ip-addr* | IP address of the remote device. |
| *hostname* | Hostname of the remote device. |
| **port** *port-num* | TCP port number on which the TCP server on the remote device listens for Telnet connections. |

**Defaults:** MSS attempts to establish Telnet connections with TCP port 23 by default.

**Access:** Enabled.

**Usage:** To end a Telnet session from the remote device, press Ctrl+t or type exit in the management session on the remote device. To end a client session from the local device, use the **clear sessions telnet client** command.

If the configuration of the switch from which you enter the **telnet** command has an ACL that denies Telnet client traffic, the ACL also denies access by the telnet command.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** In the following example, an administrator establishes a Telnet session with another switch and enters a command on the remote switch:

```
DWS-1008# telnet 10.10.10.90
Session 0 pty tty2.d Trying 10.10.10.90...
Connected to 10.10.10.90
Disconnect character is '^t'

Copyright (c) 2002, 2003 D-Link Systems, Inc.

Username:    username
Password:    password

DWS-1008-remote> show vlan
                    Admin      VLAN       Tunl                  Port
VLAN  Name          Status     State      Affin  Port   Tag    State
-----------------------------------------------------------------------------------------
1     default       Up         Up         5
                                                  1      none   Up
3     red           Up         Up         5
4     backbone      Up         Up         5
                                                  7      none   Up
                                                  8      none   Up
```

When the administrator presses Ctrl+t to end the Telnet connection, the management session returns to the local DWS prompt:

```
DWS-1008-remote> Session 0 pty tty2.d terminated tt name tty2.d
DWS-1008#
```

**See Also:**
- clear sessions
- show sessions


Download from Www.Somanuals.com. All Manuals Search And Download.

# traceroute

Traces the route to an IP host.

**Syntax: traceroute** *host* **[dnf] [no-dns] [port** *port-num***] [queries** *num***] [size** *size***] [ttl** *hops***] [wait** *ms***]**

| | |
|---|---|
| *host* | IP address, hostname, or alias of the destination host. Specify the IP address in dotted decimal notation. |
| **dnf** | Sets the Do Not Fragment bit in the ping packet to prevent the packet from being fragmented. |
| **no-dns** | Prevents MSS from performing a DNS lookup for each hop to the destination host. |
| **port** *port-num* | TCP port number listening for the traceroute probes. |
| **queries** *num* | Number of probes per hop. |
| **size** *size* | Probe packet size in bytes. You can specify from 40 through 1460. |
| **ttl** *hops* | Maximum number of hops, which can be from 1 through 255. |
| **wait** *ms* | Probe wait in milliseconds. You can specify from 1 through 100,000. |

**Defaults:**

- dnf—Disabled
- no-dns—Disabled
- port—33434
- queries—3
- size—38
- ttl—30
- wait—5000

**Access:** All.

**Usage:** To stop a traceroute command that is in progress, press Ctrl+C.

**Examples:** The following example traces the route to host server1:

```
DWS-1008# traceroute server1
traceroute to server1.example.com (192.168.22.7), 30 hops max, 38 byte packets
1 engineering-1.example.com (192.168.192.206) 2 ms 1 ms 1 ms
2 engineering-2.example.com (192.168.196.204) 2 ms 3 ms 2 ms
3 gateway_a.example.com (192.168.1.201) 6 ms 3 ms 3 ms
4 server1.example.com (192.168.22.7) 3 ms * 2 ms
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The first row of the display indicates the target host, the maximum number of hops, and the packet size. Each numbered row displays information about one hop. The rows are displayed in the order in which the hops occur, beginning with the hop closest to the switch.

The row for a hop lists the total time in milliseconds for each ICMP packet to reach the router or host, plus the time for the ICMP Time Exceeded message to return to the host.

An exclamation point (!) following any of these values indicates that the Port Unreachable message returned by the destination has a maximum hop count of 0 or 1. This can occur if the destination uses the maximum hop count value from the arriving packet as the maximum hop count in its ICMP reply. The reply does not arrive at the source until the destination receives a traceroute packet with a maximum hop count equal to the number of hops between the source and destination.

An asterisk (*) indicates that the timeout period expired before MSS received a Time Exceeded message for the packet.

If Traceroute receives an ICMP error message other than a Time Exceeded or Port Unreachable message, MSS displays one of the error codes described in the table below instead of displaying the round-trip time or an asterisk (*).

The table below describes the traceroute error messages.

| Field | Description |
|---|---|
| !N | No route to host. The network is unreachable. |
| !H | No route to host. The host is unreachable. |
| !P | Connection refused. The protocol is unreachable. |
| !F | Fragmentation needed but Do Not Fragment (DNF) bit was set. |
| !S | Source route failed. |
| !A | Communication administratively prohibited. |
| ? | Unknown error occurred. |

**See Also:**
• ping


Download from Www.Somanuals.com. All Manuals Search And Download.

# AAA Commands

Use authentication, authorization, and accounting (AAA) commands to provide a secure network connection and a record of user activity. Location policy commands override any virtual LAN (VLAN) or security ACL assignment by AAA or the local database to help you control access locally.

This chapter presents AAA commands alphabetically. Use the following table to locate commands in this chapter based on their use.


| | |
|---|---|
| **Authentication** | set authentication console on page 187<br>set authentication admin on page 186<br>set authentication dot1x on page 189<br>set authentication mac on page 192<br>set authentication proxy on page 194<br>clear authentication admin on page 172<br>clear authentication console on page 172<br>clear authentication dot1x on page 173<br>clear authentication mac on page 174<br>clear authentication proxy on page 174<br>clear authentication web on page 175 |
| **Local Authorization for Password Users** | set user on page 206<br>clear user on page 179<br>set user attr on page 207<br>clear user attr on page 180<br>set usergroup on page 208<br>clear usergroup on page 181<br>set user group on page 208<br>clear user group on page 180<br>clear usergroup attr on page 182 |
| **Local Authorization for MAC Users** | set mac-user on page 200<br>clear mac-user on page 176<br>set mac-user attr on page 200<br>clear mac-user attr on page 176<br>set mac-usergroup attr on page 205<br>clear mac-usergroup attr on page 178<br>clear mac-user group on page 177<br>clear mac-usergroup on page 178 |
| **Web authorization** | set web-portal on page 209 |
| **Accounting** | set accounting {admin \| console} on page 182<br>set accounting {dot1x \| mac \| web \| last-resort} on page 183<br>set accounting system on page 185<br>show accounting statistics on page 212<br>clear accounting on page 171 |
| **AAA information** | show aaa on page 210 |
| **Location Policy** | set location policy on page 197<br>show location policy on page 213<br>clear location policy on page 175 |




Download from Www.Somanuals.com. All Manuals Search And Download.

# clear accounting

Removes accounting services for specified wireless users with administrative access or network access.

**Syntax: clear accounting {admin | dot1x | system} {***user-glob***}**

**admin** Users with administrative access to the switch through a console connection or through a Telnet or Web View connection.

**dot1x** Users with network access through the switch. Users with network access are authorized to use the network through either an IEEE 802.1X method or their media access control (MAC) address.

**system** Disables sending of Accounting-On and Accounting-Off messages to a RADIUS server, if previously enabled. When this command is entered, an Accounting-Off message is generated and sent to the server or server group specified with the **set accounting system** command.

*user-glob* Single user or set of users with administrative access or network access.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character— either an at sign (@) or a period (.).

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes accounting services for authorized network user *Nin*:

```
DWS-1008# clear accounting dot1x Nin
success: change accepted.
```

**See Also:**
- set accounting {admin | console}
- set accounting system
- show accounting statistics


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear authentication admin

Removes an authentication rule for administrative access through Telnet or Web View.

**Syntax: clear authentication admin** *user-glob*

*user-glob* A single user or set of users.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an at sign (@) or a period (.).

**Defaults:** None.

**Access:** Enabled.

**Note:** The syntax descriptions for the **clear authentication** commands have been separated for clarity. However, the options and behavior for the **clear authentication admin** command are the same as in previous releases.

**Examples:** The following command clears authentication for administrator *Jose*:

```
DWS-1008# clear authentication admin Jose
success: change accepted.
```

**See Also:**
- clear authentication console
- clear authentication dot1x
- clear authorization mac
- clear authentication web
- set authentication admin
- show aaa

# clear authentication console

Removes an authentication rule for administrative access through the Console.

**Syntax: clear authentication console** *user-glob*

*user-glob* A single user or set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an at sign (@) or a period (.).


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** Enabled.

**Note:** The syntax descriptions for the clear authentication commands have been separated for clarity. However, the options and behavior for the **clear authentication console** command are the same as in previous releases.

**Examples:** The following command clears authentication for administrator *Regina*:

```
DWS-1008# clear authentication console Regina
success: change accepted.
```

**See Also:**
- clear authentication admin
- clear authentication dot1x
- clear authentication mac
- clear authentication web
- set authentication console
- show aaa

# clear authentication dot1x

Removes an 802.1X authentication rule.

**Syntax: clear authentication dot1x {ssid** *ssid-name* **| wired}** *user-glob*

| | |
|---|---|
| **ssid** *ssid-name* | SSID name to which this authentication rule applies. |
| **wired** | Clears a rule used for access over a switch's wired-authentication port. |
| *user-glob* | User-glob associated with the rule you are removing. |

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes 802.1X authentication for network users with usernames ending in @thiscorp.com who try to access SSID finance:

```
DWS-1008# clear authentication dot1x ssid finance *@thiscorp.com
```

**See Also:**
- clear authentication admin
- clear authentication console
- clear authentication mac
- clear authentication web
- set authentication dot1x
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear authentication mac

Removes a MAC authentication rule.

**Syntax: clear authentication mac {ssid** *ssid-name* **| wired}** *mac-addr-glob*

**ssid** *ssid-name* SSID name to which this authentication rule applies.

**wired** Clears a rule used for access over a switch's wired-authentication port.

*mac-addr-glob* MAC address glob associated with the rule you are removing.

**Access:** Enabled.

**Examples:** The following command removes a MAC authentication rule for access to SSID *thatcorp* by MAC addresses beginning with aa:bb:cc:

```
DWS-1008# clear authentication mac ssid thatcorp aa:bb:cc:*
```

**See Also:**
- clear authentication admin
- clear authentication console
- clear authentication dot1x
- clear authentication web
- set authentication mac
- show aaa

# clear authentication proxy

Removes a proxy rule for third-party AP users.

**Syntax: clear authentication proxy ssid** ssid-name user-glob

**ssid** *ssid-name* SSID name to which this authentication rule applies.

*user-glob* User-glob associated with the rule you are removing.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes the proxy rule for SSID mycorp and userglob **:

```
DWS-1008# clear authentication proxy ssid mycorp **
```

**See Also:**
- set authentication proxy
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear authentication web

Removes a WebAAA rule.

**Syntax: clear authentication web {ssid** *ssid-name* **| wired}** *user-glob*

**ssid** *ssid-name* SSID name to which this authentication rule applies.

**wired** Clears a rule used for access over a switch's wired-authentication port.

*user-glob* User-glob associated with the rule you are removing.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes WebAAA for SSID research and userglob temp*@thiscorp.com:

```
DWS-1008# clear authentication web ssid research temp*@thiscorp.com
```

**See Also:**
- clear authentication admin
- clear authentication console
- clear authentication dot1x
- clear authentication mac
- set authentication web
- show aaa

# clear location policy

Removes a rule from the location policy on a switch.

**Syntax: clear location policy** rule-number

*rule-number* Index number of a location policy rule to remove from the location policy.

**Defaults:** None.

**Access:** Enabled.

**Usage:** To determine the index numbers of location policy rules, use the show location policy command. Removing all the ACEs from the location policy disables this function on the switch.

**Examples:** The following command removes location policy rule 4 from a switch's location policy:

```
DWS-1008# clear location policy 4
success: clause 4 is removed.
```

**See Also:**
- set location policy
- show location policy


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear mac-user

Removes a user profile from the local database on the switch, for a user who is authenticated by a MAC address. (To remove a user profile in RADIUS, see the documentation for your RADIUS server.)

**Syntax: clear mac-user** *mac-addr*

*mac-addr* MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.

**Defaults:** None.

**Access:** Enabled.

**Usage:** Deleting a MAC user's profile from the database deletes the assignment of any attributes in the profile to the user.

**Examples:** The following command removes the user profile for a user at MAC address 01:02:03:04:05:06:

```
DWS-1008# clear mac-user 01:02:03:04:05:06
success: change accepted.
```

**See Also:**
- set mac-usergroup attr
- set mac-user attr
- show aaa

# clear mac-user attr

Removes an authorization attribute from the user profile in the local database on the switch, for a user who is authenticated by a MAC address. (To remove an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

**Syntax: clear mac-user** *mac-addr* **attr** *attribute-name*

*mac-addr* MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.

*attribute-name* Name of an attribute used to authorize the MAC user for a particular service or session characteristic.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes an access control list (ACL) from the profile of a user at MAC address 01:02:03:04:05:06:

```
DWS-1008# clear mac-user 01:02:03:04:05:06 attr filter-id
success: change accepted.
```

**See Also:**
- set mac-user attr
- show aaa

# clear mac-user group

Removes a user profile from a MAC user group in the local database on the switch, for a user who is authenticated by a MAC address. (To remove a MAC user group profile in RADIUS, see the documentation for your RADIUS server.)

**Syntax: clear mac-user** *mac-addr* **group**

*mac-addr* MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.

**Defaults:** None.

**Access:** Enabled.

**Usage:** Removing a MAC user from a MAC user group removes the group name from the user's profile, but does not delete the user group from the local database. To remove the group, use **clear mac-usergroup**.

**Examples:** The following command deletes the user profile for a user at MAC address 01:02:03:04:05:06 from its user group:

```
DWS-1008# clear mac-user 01:02:03:04:05:06 group
success: change accepted.
```

**See Also**:
- clear mac-usergroup
- set mac-user
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear mac-usergroup

Removes a user group from the local database on the DWS-1008 switch, for a group of users who are authenticated by a MAC address. (To delete a MAC user group in RADIUS, see the documentation for your RADIUS server.)

**Syntax: clear mac-usergroup** *group-name*

*group-name* Name of an existing MAC user group.

**Defaults:** None.

**Access:** Enabled.

**Usage:** To remove a user from a MAC user group, use the **clear mac-user group** command.

**Examples:** The following command deletes the MAC user group *eastcoasters* from the local database:

```
DWS-1008# clear mac-usergroup eastcoasters
success: change accepted.
```

**See Also:**
- clear mac-usergroup attr
- set mac-usergroup attr
- show aaa

# clear mac-usergroup attr

Removes an authorization attribute from a MAC user group in the local database on the switch, for a group of users who are authenticated by a MAC address. (To unconfigure an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

**Syntax: clear mac-usergroup** *group-name* **attr** *attribute-name*

*group-name* Name of an existing MAC user group.

*attribute-name* Name of an attribute used to authorize the MAC users in the user group for a particular service or session characteristic.

**Defaults:** None.

**Access:** Enabled.

**Usage:** To remove the group itself, use the **clear mac-usergroup** command.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command removes the members of the MAC user group *eastcoasters* from a VLAN assignment by deleting the VLAN-Name attribute from the group:

```
DWS-1008# clear mac-usergroup eastcoasters attr vlan-name
success: change accepted.
```

**See Also:**
- clear mac-usergroup
- set mac-usergroup attr
- show aaa

# clear user

Removes a user profile from the local database on the switch, for a user with a password. (To remove a user profile in RADIUS, see the documentation for your RADIUS server.)

**Syntax: clear user** *username*

*username* Username of a user with a password.

**Defaults:** None.

**Access:** Enabled.

**Usage:** Deleting the user's profile from the database deletes the assignment of any attributes in the profile to the user.

**Examples:** The following command deletes the user profile for user *Nin*:

```
DWS-1008# clear user Nin
success: change accepted.
```

**See Also:**
- set user
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear user attr

Removes an authorization attribute from the user profile in the local database on the switch, for a user with a password. (To remove an authorization attribute from a RADIUS user profile, see the documentation for your RADIUS server.)

**Syntax: clear user** *username* **attr** *attribute-name*

| | |
|---|---|
| *username* | Username of a user with a password. |
| *attribute-name* | Name of an attribute used to authorize the user for a particular service or session characteristic. |

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes the Session-Timeout attribute from Hosni's user profile:

```
DWS-1008# clear user Hosni attr session-timeout
success: change accepted.
```

**See Also:**
- set user attr
- show aaa

# clear user group

Removes a user with a password from membership in a user group in the local database on the switch. (To remove a user from a user group in RADIUS, see the documentation for your RADIUS server.)

**Syntax: clear user** *username* **group**

| | |
|---|---|
| *username* | Username of a user with a password. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** Removing the user from the group removes the group name from the user's profile, but does not delete either the user or the user group from the local database. To remove the group, use **clear usergroup**.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command removes the user Nin from the user group *Nin* is in:

```
DWS-1008# clear user Nin group
success: change accepted.
```

**See Also:**
- clear usergroup
- set user group
- show aaa

# clear usergroup

Removes a user group and its attributes from the local database on the switch, for users with passwords. (To delete a user group in RADIUS, see the documentation for your RADIUS server.)

**Syntax: clear usergroup** *group-name*

| | |
|---|---|
| *group-name* | Name of an existing user group. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** Removing a user group from the local database does not remove the user profiles of the group's members from the database.

**Examples:** The following command deletes the cardiology user group from the local database:

```
DWS-1008# clear usergroup cardiology
success: change accepted.
```

**See Also:**
- clear usergroup attr
- set usergroup
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear usergroup attr

Removes an authorization attribute from a user group in the local database on the switch. (To remove an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

**Syntax: clear usergroup** *group-name* **attr** *attribute-name*

*group-name* Name of an existing user group.

*attribute-name* Name of an attribute used to authorize all the users in the group for a particular service or session characteristic.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes the members of the user group cardiology from a network access time restriction by deleting the Time-Of-Day attribute from the group:

```
DWS-1008# clear usergroup cardiology attr time-of-day
success: change accepted.
```

**See Also:**
- clear usergroup
- set usergroup
- show aaa

# set accounting {admin | console}

Sets up accounting services for specified wireless users with administrative access, and defines the accounting records and where they are sent.

**Syntax: set accounting {admin | console}** {*user-glob*} **{start-stop | stop-only}** *method1* [*method2*] [*method3*] [*method4*]

admin Users with administrative access to the switch through Telnet or Web View.

console Users with administrative access to the switch through a console connection.

*user-glob* Single user or set of users with administrative access or network access.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globs” on page 6.)


Download from Www.Somanuals.com. All Manuals Search And Download.

*start-stop* Sends accounting records at the start and end of a network session.

*stop-only* Sends accounting records only at the end of a network session.

*method1-4* At least one of up to four methods that MSS uses to process accounting records. Specify one or more of the following methods in priority order. If the first method does not succeed, MSS tries the second method, and so on.

A method can be one of the following:

- **local**—Stores accounting records in the local database on the switch. When the local accounting storage space is full, MSS overwrites older records with new ones.

- **server-group-name**—Stores accounting records on one or more Remote Authentication Dial-In User Service (RADIUS) servers. You can also enter the names of existing RADIUS server groups as methods.

**Defaults:** Accounting is disabled for all users by default.

**Access:** Enabled.

**Usage:** For network users with start-stop accounting whose records are sent to a RADIUS server, MSS sends interim updates to the RADIUS server when the user roams.

**Examples:** The following command issues start-and-stop accounting records at the local database for administrator *Natasha*, when she accesses the switch using Telnet or Web View:

```
DWS-1008# set accounting admin Natasha start-stop local
success: change accepted.
```

**See Also:**
- clear accounting
- show accounting statistics

# set accounting {dot1x | mac | web | last-resort}

Sets up accounting services for specified wireless users with network access, and defines the accounting records and where they are sent.

**Syntax: set accounting {dot1x | mac | web | last-resort} {ssid** *ssid-name* **| wired}**
**{***user-glob* **|** *mac-addr-glob***} {start-stop | stop-only}**
*method1* **[***method2***] [***method3***] [***method4***]**


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| **dot1x** | Users with network access through the switch who are authenticated by 802.1X. |
| **mac** | Users with network access through the switch who are authenticated by MAC authentication. |
| **web** | Users with network access through the switch who are authenticated by WebAAA. |
| **ssid** *ssid-name* | SSID name to which this accounting rule applies. To apply the rule to all SSIDs, type any. |
| **wired** | Applies this accounting rule specifically to users who are authenticated on a wired authentication port. |
| *user-glob* | Single user or set of users with administrative access or network access.<br><br>Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globs” on page 6.)<br><br>**Note:** This option does not apply if mac or last-resort is specified. For mac, specify a mac-addr-glob. |
| *mac-addr-glob* | A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*) character to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 7.) This option applies only when mac is specified. |
| **start-stop** | Sends accounting records at the start and end of a network session. |
| **stop-only** | Sends accounting records only at the end of a network session. |
| *method1-4* | At least one of up to four methods that MSS uses to process accounting records. Specify one or more of the following methods in priority order. If the first method does not succeed, MSS tries the second method, and so on.<br><br>A method can be one of the following:<br><br>• **local**—Stores accounting records in the local database on the switch. When the local accounting storage space is full, MSS overwrites older records with new ones.<br><br>• **server-group-name**—Stores accounting records on one or more Remote Authentication Dial-In User Service (RADIUS) servers. You can also enter the names of existing RADIUS server groups as methods. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** Accounting is disabled for all users by default.

**Access:** Enabled.

**Usage:** For network users with start-stop accounting whose records are sent to a RADIUS server, MSS sends interim updates to the RADIUS server when the user roams.

**Examples:** The following command issues stop-only records to the RADIUS server group *sg2* for network user *Nin*, who is authenticated by 802.1X:

```
DWS-1008# set accounting dot1x Nin stop-only sg2
success: change accepted.
```

**See Also:**
- clear accounting
- show accounting statistics

# set accounting system

Configures MSS to send Accounting-On and Accounting-Off messages to a specified RADIUS server group.

**Syntax: set accounting system** *method1* **[***method2***] [***method3***] [***method4***]**

*method1-4* At least one of up to four methods that MSS uses to process accounting records. Specify one or more methods in priority order. If the first method does not succeed, MSS tries the second method, and so on.

**Note:** The local method is not valid for this command.

**Defaults:** By default MSS does not send Accounting-On or Accounting-Off messages.

**Access:** Enabled.

**Usage:** Use this command to configure MSS to send an Accounting-On message (Acct-Status-Type = 7) to a RADIUS server when the switch starts, and an Accounting-Off message (Acct-Status-Type = 8) to the RADIUS server when the switch is adminstratively shut down.

When you enable this command, an Accounting-On message is generated and sent to the specified server or server group. Subsequent Accounting-On messages are generated each time the switch starts. When the switch is administratively shut down, an Accounting-Off message is generated.

Accounting-Off messages are sent only when the switch is administratively shut down, not when a critical failure causes the switch to reset. The switch does not wait for a RADIUS server to acknowledge the Accounting-Off message; the switch makes one attempt to send the Accounting-Off message, then shuts down.

**Examples:** The following command causes Accounting-On and Accounting-Off messages to be sent to RADIUS server group *shorebirds*:

```
DWS-1008# set accounting system shorebirds
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set authentication admin

Configures authentication and defines where it is performed for specified users with administrative access through Telnet or Web View.

**Syntax: set authentication admin** *user-glob method1* **[***method2***] [***method3***] [***method4***]**

*user-glob* Single user or set of users with administrative access over the network through Telnet or Web View. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globs” on page 6.)

*method1-4* At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

A method can be one of the following:

- **local**—Uses the local database of usernames and user groups on the switch for authentication.
- **server-group-name**—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.
- **none**—For users with administrative access only, MSS performs no authentication, but prompts for a username and password and accepts any combination of entries, including blanks.

**Note:** The authentication method none you can specify for administrative access is different from the fallthru authentication type none, which applies only to network access. The authentication method none allows access to the switch by an administrator. The fallthru authentication type none denies access to a network user. For more information, see “Usage.”

**Defaults:** By default, authentication is deactivated for all admin users. The default authentication method in an admin authentication rule is local. MSS checks the local database for authentication.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** You can configure different authentication methods for different groups of users. (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 7.)

If you specify multiple authentication methods in the set authentication console command, MSS applies them in the order in which they appear in the command, with these results:

- If the first method responds with pass or fail, the evaluation is final.
- If the first method does not respond, MSS tries the second method, and so on.
- However, if local appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local database and sends an authentication request to the RADIUS server group.

**Note:** If a AAA rule specifies local as a secondary AAA method, to be used if the RADIUS servers are unavailable, and MSS authenticates a client with the local method, MSS starts again at the beginning of the method list when attempting to authorize the client. This can cause unexpected delays during client processing and can cause the client to time out before completing logon.

**Examples:** The following command configures administrator *Jose*, who connects via Telnet, for authentication on RADIUS server group *sg3*:

```
DWS-1008# set authentication admin Jose sg3
success: change accepted.
```

**See Also:**
- clear authentication admin
- set authentication console
- set authentication dot1x
- set authentication mac
- set authentication web
- show aaa

# set authentication console

Configures authentication and defines where it is performed for specified users with administrative access through a console connection.

**Syntax: set authentication console** *user-glob method1* **[***method2***] [***method3***] [***method4***]**


Download from Www.Somanuals.com. All Manuals Search And Download.

*user-glob* Single user or set of users with administrative access over the network through Telnet or Web View. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globs” on page 6.)

*method1-4* At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

A method can be one of the following:

- **local**—Uses the local database of usernames and user groups on the switch for authentication.
- **server-group-name**—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.
- **none**—For users with administrative access only, MSS performs no authentication, but prompts for a username and password and accepts any combination of entries, including blanks.

**Note:** The authentication method **none** you can specify for administrative access is different from the fallthru authentication type none, which applies only to network access. The authentication method none allows access to the switch by an administrator. The fallthru authentication type **none** denies access to a network user. For more information, see “Usage.”

**Defaults:** By default, authentication is deactivated for all console users, and the default authentication method in a console authentication rule is none. MSS requires no username or password, by default. These users can press Enter at the prompts for administrative access.

**Note:** D-Link recommends that you change the default setting unless the switch is in a secure physical location.

**Access:** Enabled.

**Note:** The syntax descriptions for the set authentication commands have been separated for clarity. However, the options and behavior for the **set authentication console** command are the same as in previous releases.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** You can configure different authentication methods for different groups of users. (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 7.)

If you specify multiple authentication methods in the **set authentication console** command, MSS applies them in the order in which they appear in the command, with these results:

- If the first method responds with pass or fail, the evaluation is final.
- If the first method does not respond, MSS tries the second method, and so on.
- However, if local appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local database and sends an authentication request to the RADIUS server group.

**Examples:** To set the console port so that it does not enforce username-password authentication for administrators, type the following command:

```
DWS-1008# set authentication console * none
success: change accepted.
```

**See Also:**
- clear authentication console
- set authentication admin
- set authentication dot1x
- set authentication mac
- set authentication web
- show aaa

# set authentication dot1x

Configures authentication and defines how and where it is performed for specified wireless or wired authentication clients who use an IEEE 802.1X authentication protocol to access the network through the switch.

**Syntax: set authentication dot1x {ssid** *ssid-name* **| wired}** *user-glob* **[bonded] protocol** *method1* **[***method2***] [***method3***] [***method4***]**

**ssid** *ssid-name* — SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type any.

**wired** — Applies this authentication rule specifically to users connected to a wired authentication port.

*user-glob* — A single user or a set of users with 802.1X network access. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globs” on page 6.)


Download from Www.Somanuals.com. All Manuals Search And Download.

**bonded** Enables Bonded Auth™ (bonded authentication). When this feature is enabled, MSS authenticates the user only if the machine the user is on has already been authenticated.

**protocol** Protocol used for authentication. Specify one of the following:

- **eap-md5**—Extensible Authentication Protocol (EAP) with message-digest algorithm 5. For wired authentication clients:
  - Uses challenge-response to compare hashes
  - Provides no encryption or integrity checking for the connection

  **Note:** The **eap-md5** option does not work with Microsoft® wired authentication clients.

- **eap-tls**—EAP with Transport Layer Security (TLS):
  - Provides mutual authentication, integrity-protected negotiation, and key exchange
  - Requires X.509 public key certificates on both sides of the connection
  - Provides encryption and integrity checking for the connection
  - Cannot be used with RADIUS server authentication (requires user information to be in the switch's local database)

- **peap-mschapv2**—Protected EAP (PEAP) with Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP-V2). For wireless clients:
  - Uses TLS for encryption and data integrity checking and server-side authentication
  - Provides MS-CHAP-V2 mutual authentication
  - Only the server side of the connection needs a certificate.

  The wireless client authenticates using TLS to set up an encrypted session. Then MS-CHAP-V2 performs mutual authentication using the specified AAA method.

- **pass-through**—MSS sends all the EAP protocol processing to a RADIUS server.


Download from Www.Somanuals.com. All Manuals Search And Download.

*method1-4* At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

A method can be one of the following:

- **local**—Uses the local database of usernames and user groups on the switch for authentication.
- **server-group-name**—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.
- **none**—For users with administrative access only, MSS performs no authentication, but prompts for a username and password and accepts any combination of entries, including blanks.

**Defaults:** By default, authentication is unconfigured for all clients with network access through AP ports or wired authentication ports on the switch. Connection, authorization, and accounting are also disabled for these users. Bonded authentication is disabled by default.

**Access:** Enabled.

**Usage:** You can configure different authentication methods for different groups of users by "globbing." (For details, see "User Globs" on page 6.)

You can configure a rule either for wireless access to an SSID, or for wired access through a switch's wired authentication port. If the rule is for wireless access to an SSID, specify the SSID name or specify any to match on all SSID names. If the rule is for wired access, specify wired instead of an SSID name. You cannot configure client authentication that uses both the EAP-TLS protocol and one or more RADIUS servers. EAP-TLS authentication is supported only on the local database.

If you specify multiple authentication methods in the **set authentication dot1x** command, MSS applies them in the order in which they appear in the command, with these results:

- If the first method responds with pass or fail, the evaluation is final.
- If the first method does not respond, MSS tries the second method, and so on.
- However, if local appears first, followed by a RADIUS server group, MSS overrides any failed searches in the local database and sends an authentication request to the server group.

If the user does not support 802.1X, MSS attempts to perform MAC authentication for the user. In this case, if the switch's configuration contains a **set authentication mac** command that matches the SSID the user is attempting to access and the user's MAC address, MSS uses the method specified by the command. Otherwise, MSS uses local MAC authentication by default.


Download from Www.Somanuals.com. All Manuals Search And Download.

If the username does not match an authentication rule for the SSID the user is attempting to access, MSS uses the fallthru authentication type configured for the SSID, which can be last-resort, web-portal (for WebAAA), or none.

**Examples:** The following command configures EAP-TLS authentication in the local database for SSID mycorp and 802.1X client *Geetha*:

```
DWS-1008# set authentication dot1x ssid mycorp Geetha eap-tls local
success: change accepted.
```

The following command configures PEAP-MS-CHAP-V2 authentication at RADIUS server groups sg1 through sg3 for all 802.1X clients at example.com who want to access SSID examplecorp:

```
DWS-1008# set authentication dot1x ssid examplecorp *@example.com
peap-mschapv2 sg1 sg2 sg3
success: change accepted.
```

**See Also:**
- clear authentication dot1x
- set authentication admin
- set authentication console
- set authentication mac
- set authentication web
- set service-profile auth-fallthru
- show aaa

# set authentication mac

Configures authentication and defines where it is performed for specified non-802.1X users with network access through a media access control (MAC) address.

**Syntax: set authentication mac {ssid** *ssid-name* **| wired}** *mac-addr-glob method1* **[***method2***] [***method3***] [***method4***]**

| | |
|---|---|
| **ssid** *ssid-name* | SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type any. |
| **wired** | Applies this authentication rule specifically to users connected to a wired authentication port. |
| *mac-addr-glob* | A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*) character to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 7.) |


Download from Www.Somanuals.com. All Manuals Search And Download.

*method1-4* At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

A method can be one of the following:

- **local**—Uses the local database of usernames and user groups on the switch for authentication.
- **server-group-name**—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods. For more information, see "Usage."

**Defaults:** By default, authentication is deactivated for all MAC users, which means MAC address authentication fails by default. When using RADIUS for authentication, the default well-known password for MAC and last-resort users is dlink.

**Access:** Enabled.

**Usage:** You can configure different authentication methods for different groups of MAC addresses by "globbing." (For details, see "User Globs, MAC Address Globs, and VLAN Globs" on page 7.)

If you specify multiple authentication methods in the **set authentication mac** command, MSS applies them in the order in which they appear in the command, with these results:

- If the first method responds with pass or fail, the evaluation is final.
- If the first method does not respond, MSS tries the second method, and so on.
- However, if local appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local database and sends an authentication request to the RADIUS server group.

If the switch's configuration contains a set authentication mac command that matches the SSID the user is attempting to access and the user's MAC address, MSS uses the method specified by the command. Otherwise, MSS uses local MAC authentication by default.

If the username does not match an authentication rule for the SSID the user is attempting to access, MSS uses the fallthru authentication type configured for the SSID, which can be last-resort, web-portal (for WebAAA), or none.

Examples: To use the local database to authenticate all users who access the *mycorp2* SSID by their MAC address, type the following command:

```
DWS-1008# set authentication ssid mycorp2 mac ** local
success: change accepted.
```

**See Also:**
- clear authentication mac
- set authentication admin
- set authentication console
- set authentication dot1x
- set authentication web
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# set authentication proxy

Configures a proxy authentication rule for a third-party AP's wireless users.

**Syntax: set authentication proxy ssid** *ssid-name user-glob* **radius-server-group**

| | |
|---|---|
| **ssid** *ssid-name* | SSID name to which this authentication rule applies. |
| *user-glob* | A single user or a set of users.<br><br>Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see "User Globs" on page 6.) |
| *radius-server-group* | A group of RADIUS servers used for authentication. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** AAA for third-party AP users has additional configuration requirements.

**Examples:** The following command configures a proxy authentication rule that matches on all usernames associated with SSID mycorp. MSS uses RADIUS server group *srvrgrp1* to proxy RADIUS requests and hence to authenticate and authorize the users.

```
DWS-1008# set authentication proxy ssid mycorp ** srvrgrp1
```

**See Also:**
- clear authentication proxy
- set radius proxy client
- set radius proxy port


Download from Www.Somanuals.com. All Manuals Search And Download.

# set authentication web

Configures an authentication rule to allow a user to log in to the network using a web page served by the switch. The rule can be activated if the user is not otherwise granted or denied access by 802.1X, or granted access by MAC authentication.

**Syntax: set authentication web {ssid** *ssid-name* **| wired}** *user-glob method1* **[***method2***] [***method3***] [***method4***]**

*user-glob* A single user or a set of users.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.).

**ssid** *ssid-name* SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type any.

**wired** Applies this authentication rule specifically to users connected to a wired authentication port.

*method1-4* At least one and up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them. A method can be one of the following:

- **local**—Uses the local database of usernames and user groups on the switch for authentication.
- **server-group-name**—Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods. RADIUS servers cannot be used with the EAP-TLS protocol. For more information, see “Usage.”

**Defaults:** By default, authentication is unconfigured for all clients with network access through AP ports or wired authentication ports on the switch. Connection, authorization, and accounting are also disabled for these users. Access Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** You can configure different authentication methods for different groups of users by "globbing."

You can configure a rule either for wireless access to an SSID, or for wired access through a switch's wired authentication port. If the rule is for wireless access to an SSID, specify the SSID name or specify any to match on all SSID names. If the rule is for wired access, specify wired instead of an SSID name.

If you specify multiple authentication methods in the **set authentication web** command, MSS applies them in the order in which they appear in the command, with these results:

- If the first method responds with pass or fail, the evaluation is final.
- If the first method does not respond, MSS tries the second method, and so on.
- However, if local appears first, followed by a RADIUS server group, MSS overrides any failed searches in the local database and sends an authentication request to the server group.

MSS uses a WebAAA rule only under the following conditions:

- The client is not denied access by 802.1X or does not support 802.1X.
- The client's MAC address does not match a MAC authentication rule.
- The fallthru type is web-portal. (For a wireless authentication rule, the fallthru type is specified by the **set service-profile auth-fallthru** command.

For a wired authentication rule, the type is specified by the auth-fall-thru option of the set port type wired-auth command.)

**Examples:** The following command configures a WebAAA rule in the local database for SSID ourcorp and userglob rnd*:

```
DWS-1008# set authentication web ssid ourcorp rnd* local
success: change accepted.
```

**See Also:**
- clear authentication web
- set authentication admin
- set authentication console
- set authentication dot1x
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# set location policy

Creates and enables a location policy on a switch. A location policy enables you to locally set or change authorization attributes for a user after the user is authorized by AAA, without making changes to the AAA server.

**Syntax: set location policy deny if {ssid** *operator ssid-name* **| vlan** *operator vlan-glob* **| user** *operator user-glob* **| port** *port-list* **| dap** *dap-num***} [before** *rule-number* **| modify** *rule-number***]**

**Syntax: set location policy permit {vlan** *vlan-name* **| inacl** *inacl-name* **| outacl** *outacl-name***} if {ssid** *operator ssid-name* **| vlan** *operator vlan-glob* **| user** *operator user-glob* **| port** *port-list* **| dap** *dap-num***} [before** *rule-number* **| modify** *rule-number***]**

**deny** Denies access to the network to users with characteristics that match the location policy rule.

**permit** Allows access to the network or to a specified VLAN, and/or assigns a particular security ACL to users with characteristics that match the location policy rule.

**Actionoptions**—For a permit rule, MSS changes the attributes assigned to the user to the values specified by the following options:

**vlan** *vlan-name* Name of an existing VLAN to assign to users with characteristics that match the location policy rule.

**inacl** *inacl-name* Name of an existing security ACL to apply to packets sent to the switch with characteristics that match the location policy rule. Optionally, you can add the suffix .in to the name.

**outacl** *outacl-name* Name of an existing security ACL to apply to packets sent from the switch with characteristics that match the location policy rule.

Optionally, you can add the suffix .out to the name.

**Condition options**—MSS takes the action specified by the rule if all conditions in the rule are met. You can specify one or more of the following conditions:

**ssid** *operator ssid-name* SSID with which the user is associated. The operator must be eq, which applies the location policy rule to all users associated with the SSID. Asterisks (wildcards) are not supported in SSID names. You must specify the complete SSID name.

**vlan** *operator vlan-glob* VLAN-Name attribute assigned by AAA and condition by which to determine if the location policy rule applies.


Download from Www.Somanuals.com. All Manuals Search And Download.

Replace operator with one of the following operands:

• **eq**—Applies the location policy rule to all users assigned VLAN names matching vlan-glob.
• **neq**—Applies the location policy rule to all users assigned VLAN names not matching vlan-glob.

For vlan-glob, specify a VLAN name, use the double-asterisk wildcard character (**) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an at sign (@) or a period (.). (For details, see "VLAN Globs" on page 6.)

**user** *operator user-glob* — Username and condition by which to determine if the location policy rule applies. Replace operator with one of the following operands:

- **eq**—Applies the location policy rule to all usernames matching user-glob.
- **neq**—Applies the location policy rule to all usernames not matching user-glob.

For user-glob, specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an at sign (@) or a period (.). (For details, see "User Globs" on page 6.)

**before** *rule-number* — Inserts the new location policy rule in front of another rule in the location policy. Specify the number of the existing location policy rule. (To determine the number, use the **show location policy** command.)

**modify** *rule-number* — Replaces the rule in the location policy with the new rule. Specify the number of the existing location policy rule. (To determine the number, use the show location policy command.)

**port** *port-list* — List of physical port(s) by which to determine if the location policy rule applies.

**Defaults:** By default, users are permitted VLAN access and assigned security ACLs according to the VLAN-Name and Filter-Id attributes applied to the users during normal authentication and authorization.

**Access:** Enabled.

**Usage:** Only a single location policy is allowed per DWS-1008 switch. The location policy can contain up to 150 rules. Once configured, the location policy becomes effective immediately. To disable location policy operation, use the **clear location policy** command.


Download from Www.Somanuals.com. All Manuals Search And Download.

Conditions within a rule are ANDed. All conditions in the rule must match in order for MSS to take the specified action. If the location policy contains multiple rules, MSS compares the user information to the rules one at a time, in the order the rules appear in the switch's configuration file, beginning with the rule at the top of the list. MSS continues comparing until a user matches all conditions in a rule or until there are no more rules.

The order of rules in the location policy is important to ensure users are properly granted or denied access. To position rules within the location policy, use before rule-number and modify rule-number in the **set location policy** command, and the clear location policy rule-number command.

When applying security ACLs:

- Use inacl inacl-name to filter traffic that enters the switch from users via an access port or wired authentication port, or from the network via a network port.
- Use outacl outacl-name to filter traffic sent from the switch to users via an AP access port or wired authentication port, or from the network via a network port.
- You can optionally add the suffixes .in and .out to inacl-name and outacl-name so that they match the names of security ACLs stored in the local database.

**Examples:** The following command denies network access to all users at *.theirfirm.com, causing them to fail authorization:

DWS-1008# **set location policy deny if user eq *.theirfirm.com**

The following command authorizes access to the *guest_1* VLAN for all users who are not at *.wodefirm.com:

DWS-1008# **set location policy permit vlan guest_1 if user neq *.wodefirm.com**

The following command authorizes users at *.ny.ourfirm.com to access the bld4.tac VLAN instead, and applies the security ACL tac_24 to the traffic they receive:

DWS-1008# **set location policy permit vlan bld4.tac outacl tac_24**
**if user eq *.ny.ourfirm.com**

The following command authorizes access to users on VLANs with names matching bld4.* and applies security ACLs svcs_2 to the traffic they send and svcs_3 to the traffic they receive:

DWS-1008# **set location policy permit inacl svcs_2 outacl svcs_3 if vlan eq bldg4.***

The following command authorizes users entering the network on ports 2 through 4 and port 6 to use the *floor2* VLAN, overriding any settings from AAA:

DWS-1008# **set location policy permit vlan floor2 if port 2-4,6**

The following command places all users who are authorized for SSID *tempvendor_a* into VLAN *kiosk_1*:

DWS-1008# **set location policy permit vlan kiosk_1 if ssid eq tempvendor_a**
success: change accepted.


Download from Www.Somanuals.com. All Manuals Search And Download.

# set mac-user

Configures a user profile in the local database on the switch for a user who can be authenticated by a MAC address, and optionally adds the user to a MAC user group. (To configure a MAC user profile in RADIUS, see the documentation for your RADIUS server.)

**Syntax: set mac-user** *mac-addr* **[group** *group-name***]**

| | |
|---|---|
| *mac-addr* | MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros. |
| *group-name* | Name of an existing MAC user group. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** MSS does not require MAC users to belong to user groups.

Users authenticated by MAC address can be authenticated only for network access through the switch. MSS does not support passwords for MAC users.

**Examples:** The following command creates a user profile for a user at MAC address 01:02:03:04:05:06 and assigns the user to the *eastcoasters* user group:

```
DWS-1008# set mac-user 01:02:03:04:05:06 group eastcoasters
success: change accepted.
```

**See Also:**
- clear mac-user
- show aaa

# set mac-user attr

Assigns an authorization attribute in the local database on the switch to a user who is authenticated by a MAC address. (To assign authorization attributes through RADIUS, see the documentation for your RADIUS server.)

**Syntax: set mac-user** *mac-addr* **attr attribute-name** *value*

| | |
|---|---|
| *mac-addr* | MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros. |
| **attribute-name** *value* | Name and value of an attribute you are using to authorize the MAC user for a particular service or session characteristic. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** Enabled.

**Usage:** To change the value of an attribute, enter set mac-user attr with the new value. To delete an attribute, use **clear mac-user attr**.

You can assign attributes to individual MAC users and to MAC user groups. If attributes are configured for a MAC user and also for the group the MAC user is in, the attributes assigned to the individual MAC user take precedence for that user. For example, if the start-date attribute configured for a MAC user is sooner than the start-date configured for the MAC user group the user is in, the MAC user's network access can begin as soon as the user start-date. The MAC user does not need to wait for the MAC user group's start date.

| Attribute | Description | Valid Value(s) |
|---|---|---|
| encryption-type | Type of encryption required for access by the client. Clients who attempt to use an unauthorized encryption method are rejected.<br><br>**Note:** Encryption-Type is a D-Link vendor-specific attribute (VSA). The vendor ID is 14525, and the vendor type is 3. | One of the following numbers that identifies an encryption algorithm:<br>• 1—AES_CCM (Advanced Encryption Standard using Counter with CBC-MAC)<br>• 2—Reserved<br>• 4—TKIP (Temporal Key Integrity Protocol)<br>• 8—WEP_104 (the default) (Wired-Equivalent Privacy protocol using 104 bits of key strength)<br>• 16—WEP_40 (Wired-Equivalent Privacy protocol using 40 bits of key strength)<br>• 32—NONE (no encryption)<br>• 64—Static WEP In addition to these values, you can specify a sum of them for a combination of allowed encryption types. For example, to specify WEP_104 and WEP_40, use 24. |
| end-date | Date and time after which the user is no longer allowed to be on the network. | Date and time, in the following format:<br>YY/MM/DD-HH:MM Y<br>You can use end-date alone or with start-date. You also can use start-date, end-date, or both in conjunction with time-of-day. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Attribute | Description | Valid Value(s) |
|---|---|---|
| filter-id (network access mode only) | Security access control list (ACL), to permit or deny traffic received (input) or sent (output) by the switch. | Name of an existing security ACL, up to 253 alphanumeric characters, with no tabs or spaces.<br>• Use acl-name.in to filter traffic that enters the switch from users via an AP access port or wired authentication port, or from the network via a network port.<br>• Use acl-name.out to filter traffic sent from the switch to users via an AP access port or wired authentication port, or from the network via a network port.<br>**Note:** If the Filter-Id value returned through the authentication and authorization process does not match the name of a committed security ACL in the switch, the user fails authorization and is unable to authenticate. |
| service-type | Type of access the user is requesting. | One of the following numbers:<br>• 2—Framed; for network user access<br>• 6—Administrative; for administrative access to the switch, with authorization to access the enabled (configuration) mode. The user must enter the enable command and the correct enable password to access the enabled mode.<br>• 7—NAS-Prompt; for administrative access to the nonenabled mode only. In this mode, the user can still enter the enable command and the correct enable password to access the enabled mode.<br>For administrative sessions, the switch always sends 6 (Administrative). The RADIUS server can reply with one of the values listed above. If the service-type is not set on the RADIUS server, administrative users receive NAS-Prompt access, and network users receive Framed access. |
| session-timeout (network access mode only) | Maximum number of seconds for the user's session. | Number between 0 and 4,294,967,296 seconds (approximately 136.2 years).<br>**Note:** If the global reauthentication timeout (set by the set dot1x reauth-period command) is shorter than the session-timeout, MSS uses the global timeout instead. |
| ssid (network access mode only) | SSID the user is allowed to access after authentication. | Name of the SSID you want the user to use. The SSID must be configured in a service profile, and the service profile must be used by a radio profile assigned to D-Link radios in the network. |
| start-date | Date and time at which the user becomes eligible to access the network. MSS does not authenticate the user unless the attempt to access the network occurs at or after the specified date and time, but before the end-date (if specified). | Date and time, in the following format:<br>**YY/MM/DD-HH:MM**<br>You can use start-date alone or with end-date. You also can use start-date, end-date, or both in conjunction with time-of-day. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Attribute | Description | Valid Value(s) |
|---|---|---|
| time-of-day<br>(network access mode only) | Day(s) and time(s) during which the user is permitted to log into the network. After authorization, the user's session can last until either the Time-Of-Day range or the Session-Timeout duration (if set) expires, whichever is shorter. | One of the following:<br>• never—Access is always denied.<br>• any—Access is always allowed.<br>• al—Access is always allowed.<br>• One or more ranges of values that consist of one of the following day designations (required), and a time range in hhmm-hhmm 4-digit 24-hour format (optional):<br>• mo—Monday<br>• tu—Tuesday<br>• we—Wednesday<br>• th—Thursday<br>• fr—Friday<br>• sa—Saturday<br>• su—Sunday<br>• wk—Any day between Monday and Friday<br><br>Separate values or a series of ranges (except time ranges) with commas (,) or a vertical bar (\|). Do not use spaces. The maximum number of characters is 253.<br>For example, to allow access only on Tuesdays and Thursdays between 10 a.m. and 4 p.m., specify the following:<br>**time-of-day tu1000-1600,th1000-1600**<br><br>To allow access only on weekdays between 9 a.m and 5 p.m., and on Saturdays from 10 p.m. until 2 a.m., specify the following:<br>time-of-day wk0900-1700,sa2200-0200<br><br>**Note:** You can use time-of-day in conjunction with start-date, end-date, or both. |
| url<br>(network access mode only) | URL to which the user is redirected after successful WebAAA. | Web URL, in standard format. For example: http://www.example.com<br>**Note:** You must include the http:// portion.<br>You can dynamically include any of the variables in the URL string:<br>• $u—Username<br>• $v—VLAN<br>• $s—SSID<br>• $p—Service profile name<br>To use the literal character $ or ?, use the following:<br>• $$<br>• $q |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Attribute | Description | Valid Value(s) |
|---|---|---|
| vlan-name (network access mode only) | Virtual LAN (VLAN) assignment. Note: On some RADIUS servers, you might need to use the standard RADIUS attribute Tunnel-Pvt-Group-ID, instead of VLAN-Name. | Name of a VLAN that you want the user to use. |
| acct-interim-interval | Interval in seconds between accounting updates, if start-stop accounting mode is enabled. | Number between 180 and 3,600 seconds, or 0 to disable periodic accounting updates. The switch ignores the acct-interim-interval value and issues a log message if the value is below 60 seconds. **Note:** If both a RADIUS server and the switch supply a value for the acct-interim-interval attribute, then the value from the switch takes precedence. |

**Examples:** The following command assigns input access control list (ACL) acl-03 to filter the packets from a user at MAC address 01:02:03:04:05:06:

DWS-1008# **set mac-user 01:02:03:04:05:06 attr filter-id acl-03.in**
success: change accepted.

The following command restricts a user at MAC address 06:05:04:03:02:01 to network access between 7 p.m. on Mondays and Wednesdays and 7 a.m. on Tuesdays and Thursdays:

DWS-1008# **set mac-user 06:05:04:03:02:01 attr time-of-day mo1900-1159,tu0000-0700,we1900-1159,th0000-0700**
success: change accepted.

**See Also:**
- clear mac-user attr
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# set mac-usergroup attr

Creates a user group in the local database on the switch for users who are authenticated by a MAC address, and assigns authorization attributes for the group.

(To configure a user group and assign authorization attributes through RADIUS, see the documentation for your RADIUS server.)

**Syntax: set mac-usergroup** *group-name* **attr** *attribute-name value*

| | |
|---|---|
| *group-name* | Name of a MAC user group. Specify a name of up to 32 alphanumeric characters, with no spaces. The name must begin with an alphabetic character. |
| **attribute-name** *value* | Name and value of an attribute you are using to authorize all MAC users in the group for a particular service or session characteristic. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** To change the value of an attribute, enter set mac-usergroup attr with the new value. To delete an attribute, use **clear mac-usergroup attr**.

You can assign attributes to individual MAC users and to MAC user groups. If attributes are configured for a MAC user and also for the group the MAC user is in, the attributes assigned to the individual MAC user take precedence for that user. For example, if the start-date attribute configured for a MAC user is sooner than the start-date configured for the MAC user group the user is in, the MAC user's network access can begin as soon as the user start-date. The MAC user does not need to wait for the MAC user group's start date.

**Examples:** The following command creates the MAC user group *eastcoasters* and assigns the group members to VLAN *orange*:

```
DWS-1008# set mac-usergroup eastcoasters attr vlan-name orange
success: change accepted.
```

**See Also:**
- clear mac-usergroup attr
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# set user

Configures a user profile in the local database on the switch for a user with a password. (To configure a user profile in RADIUS, see the documentation for your RADIUS server.)

**Syntax: set user** *username* **password [encrypted]** *string*

| | |
|---|---|
| *username* | Username of a user with a password. |
| **encrypted** | Indicates that the password string you entered is already in its encrypted form. If you use this option, MSS does not encrypt the displayed form of the password string, and instead displays the string exactly as you entered it. If you omit this option, MSS does encrypt the displayed form of the string. |
| **password** *string* | Password of up to 32 alphanumeric characters, with no spaces. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** The **show config** command shows the encrypted option with this command, even when you omit the option. The encrypted option appears in the configuration because MSS automatically encrypts the password when you create the user (unless you use the encrypted option when you enter the password).

Although MSS allows you to configure a user password for the special “last-resort” guest user, the password has no effect. Last-resort users can never access a switch in administrative mode and never require a password.

The only valid username of the form last-resort-* is last-resort-wired. The last-resort-wired user allows last-resort access on a wired authentication port.

**Examples:** The following command creates a user profile for user *Nin* in the local database, and assigns the password *goody*:

```
DWS-1008# set user Nin password goody
success: User Nin created
```

The following command assigns the password *chey3nne* to the admin user:

```
DWS-1008# set user admin password chey3nne
success: User admin created
```

The following command changes Nin’s password from *goody* to *29Jan04*:

```
DWS-1008# set user Nin password 29Jan04
```

**See Also:**
- clear user
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# set user attr

Configures an authorization attribute in the local database on the switch for a user with a password.
(To assign authorization attributes in RADIUS, see the documentation for your RADIUS server.)

**Syntax: set user** *username* **attr** *attribute-name value*

| | |
|---|---|
| *username* | Username of a user with a password. |
| *attribute-name value* | Name and value of an attribute you are using to authorize the user for a particular service or session characteristic. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** To change the value of an attribute, enter **set user attr** with the new value. To delete an attribute, use **clear user attr**.

You can assign attributes to individual users and to user groups. If attributes are configured for a user and also for the group the user is in, the attributes assigned to the individual user take precedence for that user. For example, if the start-date attribute conhefigured for a user is sooner than the start-date configured for the user group the user is in, the user's network access can begin as soon as the user start-date. The user does not need to wait for the user group's start date.

**Examples:** The following command assigns user Tamara to VLAN *orange*:

```
DWS-1008# set user Tamara attr vlan-name orange
success: change accepted.
```

The following command limits the days and times when user *Student1* can access the network, to 5 p.m. to 2 a.m. every weekday, and all day Saturday and Sunday:

```
DWS-1008# set user Student1 attr time-of-day Wk1700-0200,Sa,Su
success: change accepted.
```

**See Also:**
- clear user attr
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# set user group

Adds a user to a user group. The user must have a password and a profile that exists in the local database on the switch.
(To configure a user in RADIUS, see the documentation for your RADIUS server.)

**Syntax: set user** *username* **group** *group-name*

*username* Username of a user with a password.

*group-name* Name of an existing user group for password users.

**Defaults:** None.

**Access:** Enabled.

**Usage:** MSS does not require users to belong to user groups. To create a user group, user the command **set usergroup**.

**Examples:** The following command adds user *Hosni* to the cardiology user group:

```
DWS-1008# set user Hosni group cardiology
success: change accepted.
```

**See Also:**
- clear user group
- show aaa

# set usergroup

Creates a user group in the local database on the switch for users and assigns authorization attributes for the group.
(To create user groups and assign authorization attributes in RADIUS, see the documentation for your RADIUS server.)

**Syntax: set usergroup** *group-name* **attr** *attribute-name value*

*group-name* Name of a group for password users. Specify a name of up to 32 alphanumeric characters, with no spaces. The name must begin with an alphabetic character.

*attribute-name value* Name and value of an attribute you are using to authorize all users in the group for a particular service or session characteristic.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** Enabled.

**Usage:** To change the value of an attribute, enter set usergroup attr with the new value. To delete an attribute, use **clear usergroup attr**. To add a user to a group, user the command **set user group**.

You can assign attributes to individual users and to user groups. If attributes are configured for a user and also for the group the user is in, the attributes assigned to the individual user take precedence for that user. For example, if the start-date attribute configured for a user is sooner than the start-date configured for the user group the user is in, the user's network access can begin as soon as the user start-date. The user does not need to wait for the user group's start date.

**Examples:** The following command adds the user group cardiology to the local database and assigns all the group members to VLAN *crimson*:

```
DWS-1008# set usergroup cardiology attr vlan-name crimson
success: change accepted.
```

**See Also:**
- clear usergroup
- clear usergroup attr
- show aaa

# set web-portal

Globally enables or disables WebAAA on a DWS-1008 switch.

**Syntax: set web-portal {enable | disable}**

**enable** Enables WebAAA on the switch.

**disable** Disables WebAAA on the switch.

**Defaults:** Enabled.

**Access:** Enabled.

**Usage:** This command disables or reenables support for WebAAA. However, WebAAA has additional configuration requirements.

**Examples:** To disable WebAAA, type the following command:

```
DWS-1008# set web-portal disable
success: change accepted.
```

**See Also:**
- clear authentication web
- set service-profile auth-fallthru
- set user


Download from Www.Somanuals.com. All Manuals Search And Download.

# show aaa

Displays all current AAA settings.

**Syntax: show aaa**

**Defaults:** None.

**Access:** Enabled.

**Examples:** To display all current AAA settings, type the following command:

DWS-1008# **show aaa**
Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=0 key=(null) author-pass=(null)

Radius Servers

| Server | Addr | Ports | T/o | Tries | Dead | State |
|---|---|---|---|---|---|---|
| rs-3 | 198.162.1.1 | 1821 1813 | 5 | 3 | 0 | UP |
| rs-4 | 198.168.1.2 | 1821 1813 | 77 | 11 | 2 | UP |
| rs-5 | 198.162.1.3 | 1821 1813 | 42 | 23 | 0 | UP |

Server groups
sg1: rs-3
sg2: rs-4
sg3: rs-5

Web Portal:
enabled

set authentication admin Jose sg3
set authentication console * none
set authentication mac ssid mycorp * local
set authentication dot1x ssid mycorp Geetha eap-tls
set authentication dot1x ssid mycorp * peap-mschapv2 sg1 sg2 sg3
set authentication dot1x ssid any ** peap-mschapv2 sg1 sg2 sg3
set accounting dot1x Nin ssid mycorp stop-only sg2
set accounting admin Natasha start-stop local

user Nin
Password = 082c6c64060b (encrypted)
Filter-Id = acl-999.in
Filter-Id = acl-999.out

mac-user 01:02:03:04:05:06

usergroup eastcoasters
session-timeout = 99


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields that can appear in **show aaa** output.

| Field | Description |
|---|---|
| **Default Values** | RADIUS default values for all parameters. |
| **authport** | UDP port on the switch for transmission of RADIUS authorization and authentication messages. The default port is 1812. |
| **acctport** | UDP port on the switch for transmission of RADIUS accounting records. The default is port 1813. |
| **timeout** | Number of seconds the switch waits for a RADIUS server to respond before retransmitting. The default is 5 seconds. |
| **acct-timeout** | Number of seconds the switch waits for a RADIUS server to respond to an accounting request before retransmitting. The default is 5 seconds. |
| **retrans** | Number of times the switch retransmits a message before determining a RADIUS server unresponsive. The default is 3 times. |
| **deadtime** | Number of minutes the switch waits after determining a RADIUS server is unresponsive before trying to reconnect with this server. During the dead time, the RADIUS server is ignored by the switch. The default is 0 minutes. |
| **key** | Shared secret key, or password, used to authenticate to a RADIUS server. The default is no key (null). |
| **author-pass** | Password used for authorization to a RADIUS server for MAC authentication. The client's MAC address is sent as the username and the author-pass string is sent as the password. |
| **Radius Servers** | Information about active RADIUS servers. |
| **Server** | Name of each RADIUS server currently active. |
| **Addr** | IP address of each RADIUS server currently active. |
| **Ports** | UDP ports that the switch uses for authentication messages and for accounting records. |
| **T/o** | Setting of timeouts on each RADIUS server currently active. |
| **Tries** | Number of retransmissions configured for each RADIUS server currently active. The default is 3 times. |
| **Dead** | Length of time until the server is considered responsive again. |
| **State** | Current state of each RADIUS server currently active:<br>• UP (operating)<br>• DOWN (unavailable) |
| **Server groups** | Names of RADIUS server groups and member servers configured on the switch. |
| **Web Portal** | State of the WebAAA feature:<br>• enabled<br>• disabled |
| **set commands** | List of commands used to configure AAA on the switch. |
| **user and user group profiles** | List of user and user group profiles stored in the local database on the switch. |

**See Also:**

- set accounting {admin | console}
- set authentication admin
- set authentication console
- set authentication dot1x
- set authentication mac
- set authentication web


Download from Www.Somanuals.com. All Manuals Search And Download.

# show accounting statistics

Displays the AAA accounting records for wireless users. The records are stored in the local database on the switch.
(To display RADIUS accounting records, see the documentation for your RADIUS server.)

**Syntax: show accounting statistics**

**Defaults:** None.

**Access:** Enabled.

**Examples:** To display the locally stored accounting records, type the following command:

```
DWS-1008# show accounting statistics
Dec 14 00:39:48
Acct-Status-Type=STOP
Acct-Authentic=0
Acct-Multi-Session-Id=SESS-3-01f82f-520236-24bb1223
Acct-Session-Id=SESS-3-01f82f-520236-24bb1223
User-Name=vineet
AAA_ACCT_SVC_ATTR=2
Acct-Session-Time=551
Event-Timestamp=1134520788
Acct-Output-Octets=3204
Acct-Input-Octets=1691
Acct-Output-Packets=20
Acct-Input-Packets=19
AAA_VLAN_NAME_ATTR=default
Calling-Station-Id=00-06-25-12-06-38
Nas-Port-Id=3/1
Called-Station-Id=00-0B-0E-00-CC-01
AAA_SSID_ATTR=vineet-dot1x

Dec 14 00:39:53
Acct-Status-Type=START
Acct-Authentic=0
User-Name=vineet
Acct-Multi-Session-Id=SESS-4-01f82f-520793-bd779517
Acct-Session-Id=SESS-4-01f82f-520793-bd779517
Event-Timestamp=1134520793
AAA_ACCT_SVC_ATTR=2
AAA_VLAN_NAME_ATTR=default
Calling-Station-Id=00-06-25-12-06-38
Nas-Port-Id=3/1
Called-Station-Id=00-0B-0E-00-CC-01
AAA_SSID_ATTR=vineet-dot1x
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields that can appear in **show accounting statistics** output.

| Field | Description |
|---|---|
| Date and time | Date and time of the accounting record. |
| Acct-Status-Type | Type of accounting record:<br>• START<br>• STOP<br>• UPDATE |
| Acct-Authentic | Location where the user was authenticated (if authentication took place) for the session:<br>• 1—RADIUS server<br>• 2—Local database |
| User-Name | Username of a user with a password. |
| Acct-Multi-Session-Id | Unique accounting ID for multiple related sessions in a log file. |
| AAA_TTY_ATTR | For sessions conducted through a console or administrative Telnet connection, the Telnet terminal number. |
| Event-Timestamp | Time (in seconds since January 1, 1970) at which the event was triggered. (See RFC 2869 for more information.) |
| Acct-Session-Time | Number of seconds that the session has been online. |
| Acct-Output-Octets | Number of octets the switch has sent during the session. |
| Acct-Input-Octets | Number of octets the switch has received during the session. |
| Acct-Output-Packets | Number of packets the switch has sent during the session. |
| Acct-Input-Packets | Number of packets the switch has received during the session. |
| Vlan-Name | Name of the client's VLAN. |
| Calling-Station-Id | MAC address of the supplicant (client). |
| Nas-Port-Id | Number of the port and radio on the access point through which the session was conducted. |
| Called-Station-Id | MAC address of the access point through which the client reached the network. |

**See Also:**
- clear accounting
- set accounting {admin | console}
- show aaa

# show location policy

Displays the list of location policy rules that make up the location policy on a DWS-1008 switch.

**Syntax: show location policy**

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command displays the list of location policy rules in the location policy on a switch:

```
DWS-1008 show location policy
Id Clauses
-----------------------------------------------------------------
1) deny if user eq *.theirfirm.com
2) permit vlan guest_1 if vlan neq *.wodefirm.com
3) permit vlan bld4.tac inacl tac_24.in if user eq *.ny.wodefirm.com
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# Cryptography Commands

A digital certificate is a form of electronic identification for computers. The switch requires digital certificates to authenticate its communications to Web View, to WebAAA clients, and to Extensible Authentication Protocol (EAP) clients for which the switch performs all EAP processing. Certificates can be generated on the switch or obtained from a certificate authority (CA). Keys contained within the certificates allow the switch, its servers, and its wireless clients to exchange information secured by encryption.

> **Note:** If the switch does not already have certificates, MSS automatically generates the missing ones the first time you boot using MSS Version 4.2 or later. You do not need to install certificates unless you want to replace the ones automatically generated by MSS.

> **Note:** Before installing a new certificate, verify with the show timedate and show timezone commands that the switch is set to the correct date, time, and time zone. Otherwise, certificates might not be installed correctly.

| | |
|---|---|
| **Encryption Keys** | crypto generate key on page 217<br>show crypto key domain on page 226<br>show crypto key ssh on page 226 |
| **PKCS#7 Certificates** | **c**rypto generate request on page 218<br>crypto ca-certificate on page 215<br>show crypto ca-certificate on page 224<br>crypto certificate on page 216<br>show crypto certificate on page 225 |
| **PKCS#12 Certificate** | crypto otp on page 222<br>crypto pkcs12 on page 223 |
| **Self-Signed Certificate** | crypto generate self-signed on page 220 |


Download from Www.Somanuals.com. All Manuals Search And Download.

# crypto ca-certificate

Installs a certificate authority's own PKCS#7 certificate into the switch certificate and key storage area.

**Syntax: crypto ca-certificate {admin | eap | web}**
*PEM-formatted-certificate*

| | |
|---|---|
| **admin** | Stores the certificate authority's certificate that signed the administrative certificate for the switch. The administrative certificate authenticates the switch to Web View. |
| **eap** | Stores the certificate authority's certificate that signed the Extensible Authentication Protocol (EAP) certificate for the switch. The EAP certificate authenticates the switch to 802.1X supplicants (clients). |
| **web** | Stores the certificate authority's certificate that signed the WebAAA certificate for the switch. The Web certificate authenticates the switch to clients who use WebAAA. |
| *PEM-formatted-certificate* | ASCII text representation of the certificate authority PKCS#7 certificate, consisting of up to 5120 characters that you have obtained from the certificate authority. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** The Privacy-Enhanced Mail protocol (PEM) format is used for representing a PKCS#7 certificate in ASCII text. PEM uses base64 encoding to convert the certificate to ASCII text, then puts the encoded text between the following delimiters:

-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----

To use this command, you must already have obtained a copy of the certificate authority's certificate as a PKCS#7 object file. Then do the following:

1. Open the PKCS#7 object file with an ASCII text editor such as Notepad orvi.

2. Enter the **crypto ca-certificate** command on the CLI command line.

3. When MSS prompts you for the PEM-formatted certificate, paste the PKCS#7 object file onto the command line.


Download from Www.Somanuals.com. All Manuals Search And Download.

Examples The following command adds the certificate authority's certificate to switch certificate and key storage:

```
DWS-1008# crypto ca-certificate admin
Enter PEM-encoded certificate
-----BEGIN CERTIFICATE-----
MIIDwDCCA2qgAwIBAgIQL2jvuu4PO5FAQCyewU3ojANBgkqhkiG9wOBAQUFADCB
mzerMClaweVQQTTooewi\wpoer0QWNFNkj90044mbdrl1277SWQ8G7Diw
YUtrqoQplKJvxz .....
Lm8wmVYxP56M;CUAm908C2foYgOY40=
-----END CERTIFICATE-----
```

**See Also:**
• show crypto ca-certificate

# crypto certificate

Installs one of the switch's PKCS#7 certificates into the certificate and key storage area on the switch. The certificate, which is issued and signed by a certificate authority, authenticates the switch either to Web View, or to 802.1X supplicants (clients).

**Syntax: crypto certificate {admin | eap | web}** *PEM-formatted-certificate*

| | |
|---|---|
| **admin** | Stores the certificate authority's administrative certificate, which authenticates the switch to Web View. |
| **eap** | Stores the certificate authority's Extensible Authentication Protocol (EAP) certificate, which authenticates the switch to 802.1X supplicants (clients). |
| **web** | Stores the certificate authority's WebAAA certificate, which authenticates the to clients who use WebAAA. |
| *PEM-formatted-certificate* | ASCII text representation of the certificate authority PKCS#7 certificate, consisting of up to 5120 characters that you have obtained from the certificate authority. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** To use this command, you must already have generated a certificate request with the crypto generate request command, sent the request to the certificate authority, and obtained a signed copy of the switch certificate as a PKCS#7 object file. Then do the following:


Download from Www.Somanuals.com. All Manuals Search And Download.

1. Open the PKCS#7 object file with an ASCII text editor such as Notepad or vi.

2. Enter the **crypto certificate** command on the CLI command line.

3. When MSS prompts you for the PEM-formatted certificate, paste the PKCS#7 object file onto the command line.

The switch verifies the validity of the public key associated with this certificate before installing it, to prevent a mismatch between the switch's private key and the public key in the installed certificate.

**Examples:** The following command installs a certificate:

```
DWS-1008# crypto certificate admin
Enter PEM-encoded certificate
-----BEGIN CERTIFICATE-----
MIIBdTCP3wIBADA2MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQOEx
GjAYBgNVBAMU EXR1Y2hwdWJzQHRycHouY29tMIGfMAOGCSqGSIb3DQ
EBAQAA4GNADCBiQKBgQC4 .....
2L8Q9tk+G2As84QYLm8wmVY>xP56M;CUAm908C2foYgOY40=
-----END CERTIFICATE-----
```

**See Also:**
- crypto generate request
- crypto generate self-signed

# crypto generate key

Generates an RSA public-private encryption key pair that is required for a Certificate Signing Request (CSR) or a self-signed certificate. For SSH, generates an authentication key.

**Syntax: crypto generate key {admin | eap | ssh | web}**
**{128 | 512 | 1024 | 2048}**

| | |
|---|---|
| **admin** | Generates an administrative key pair for authenticating the switch to or Web View. |
| **eap** | Generates an EAP key pair for authenticating the switch to 802.1X supplicants (clients). |
| **ssh** | Generates a key pair for authenticating the switch to Secure Shell (SSH) clients. |
| **web** | Generates an administrative key pair for authenticating the switch to WebAAA clients. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| **128 \| 512 \| 1024 \| 2048** | Length of the key pair in bits.<br>**Note:** The minimum key length for SSH is 1024. The length 128 applies only to domain and is the only valid option for it. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** You can overwrite a key by generating another key of the same type.

SSH requires an SSH authentication key, but you can allow MSS to generate it automatically. The first time an SSH client attempts to access the SSH server on a switch, the switch automatically generates a 1024-byte SSH key. If you want to use a 2048-byte key instead, use the **crypto generate key ssh 2048** command to generate one.

**Examples:** To generate an administrative key, type the following command:

```
DWS-1008# crypto generate key admin 1024
key pair generated.
```

**See Also:**
• show crypto key ssh

# crypto generate request

Generates a Certificate Signing Request (CSR). This command outputs a PEM-formatted PKCS#10 text string that you can cut and paste to another location for delivery to a certificate authority.

This command generates either an administrative CSR for use with Web View or an EAP CSR for use with 802.1X clients.

**Syntax: crypto generate request {admin | eap | web}**

| | |
|---|---|
| **admin** | Generates a request for an administrative certificate to authenticate the switch to Web View. |
| **eap** | Generates a request for an EAP certificate to authenticate the switch to 802.1X supplicants (clients). |
| **web** | Generates a request for a WebAAA certificate to authenticate the switch to WebAAA clients. |

After type the command, you are prompted for the following variables:

| | |
|---|---|
| Country Name<br>*string* | (Optional) Specify the abbreviation for the country in which the switch is operating, in 2 alphanumeric characters with no spaces. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| State Name *string* | (Optional) Specify the name of the state, in up to 64 alphanumeric characters. Spaces are allowed. |
| Locality Name *string* | (Optional) Specify the name of the locality, in up to 80 alphanumeric characters with no spaces. |
| Organizational Name *string* | (Optional) Specify the name of the organization, in up to 80 alphanumeric characters with no spaces. |
| Organizational Unit *string* | (Optional) Specify the name of the organizational unit, in up to 80 alphanumeric characters with no spaces. |
| Common Name *string* | Specify a unique name for the switch, in up to 80 alphanumeric characters with no spaces. Use a fully qualified name if such names are supported on your network. This field is required. |
| Email Address *string* | (Optional) Specify your email address, in up to 80 alphanumeric characters with no spaces. |
| Unstructured Name *string* | (Optional) Specify any name, in up to 80 alphanumeric characters with no spaces. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** To use this command, you must already have generated a public-private encryption key pair with the **crypto generate key** command.

Enter **crypto generate request admin, crypto generate request eap,** or **crypto generate request web** and press Enter. When you are prompted, type the identifying values in the fields, or press Enter if the field is optional. You must enter a common name for the switch.

This command outputs a PKCS#10 text string in Privacy-Enhanced Mail protocol (PEM) format that you paste to another location for submission to the certificate authority. You then send the request to the certificate authority to obtain a signed copy of the switch certificate as a PKCS#7 object file.

**Examples:** To request an administrative certificate from a certificate authority, type the following command:

```
DWS-1008# crypto generate request admin
Country Name: US
State Name: CA
Locality Name: Pleasanton
Organizational Name: D-Link
Organizational Unit: ENG
Common Name: ENG
Email Address: admin@example.com
Unstructured Name: admin
```


Download from Www.Somanuals.com. All Manuals Search And Download.

CSR for admin is
-----BEGIN CERTIFICATE REQUEST-----
MIIBuzCCASQCAQAwezELMAkGA1UEBhMCdXMxCzAJBgNVBAgTAmNhMQswCQYDVQQH
EwJjYTELMAkGA1UEChMCY2ExCzAJBgNVBAsTAmNhMQswCQYDVQQDEwJjYTEYMBYG
CSqGSIb3DQEJARYJY2FAY2EuY29tMREwDwYJKoZIhvcNAQkCEwJjYTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA1zatpYStOjHMa0QJmWHeZPPFGQ9kBEimJKPG
bznFjAC780GcZtnJPGqnMnOKj/4NdknonT6NdCd2fBdGbuEFGNMNgZMYKGcV2JIu
tr*P*z*exECScaNlicKMYa$$_Qo621vh67RM1KTMECM6uCBB6XNypIHn1gtrrpL/
LhyGTWUCAwEAAaAAMA0GCSqGSIb3DQEBBAUAA4GBAHK5z2kfjBbV/F0b0MyC5S7K
htsw7T4SwmCij55qfUHxsRelggYcw6vJtr57jJ7wFfsMd8C50NcbJLF1nYC9OKkB
hW+5gDPAOZdOnnr591XKz3Zzyvyrktv00rcld8Fo2RtTQ3AOT9cUZqJVelO85GXJ
-----END CERTIFICATE REQUEST-----

**See Also:**
- crypto certificate
- crypto generate key

# crypto generate self-signed

Generates a self-signed certificate for either an administrative certificate for use with an EAP certificate for use with 802.1X wireless users.

**Syntax: crypto generate self-signed {admin | eap | web}**

| | |
|---|---|
| **admin** | Generates an administrative certificate to authenticate the switch to Web View. |
| **eap** | Generates an EAP certificate to authenticate the switch to 802.1X supplicants (clients). |
| **web** | Generates a WebAAA certificate to authenticate the switch to WebAAA clients. |

After type the command, you are prompted for the following variables:

| | |
|---|---|
| Country Name *string* | (Optional) Specify the abbreviation for the country in which the switch is operating, in 2 alphanumeric characters with no spaces. |
| State Name *string* | (Optional) Specify the abbreviation for the name of the state, in 2 alphanumeric characters with no spaces. |
| Locality Name *string* | (Optional) Specify the name of the locality, in up to 80 alphanumeric characters with no spaces. |
| Organizational Name *string* | (Optional) Specify the name of the organization, in up to 80 alphanumeric characters with no spaces. |
| Organizational Unit *string* | (Optional) Specify the name of the organizational unit, in up to 80 alphanumeric characters with no spaces. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| Common Name<br>*string* | Specify a unique name for the switch, in up to 80 alphanumeric characters with no spaces. Use a fully qualified name if such names are supported on your network. This field is required.<br><br>**Note:** If you are generating a WebAAA (web) certificate, use a common name that looks like a domain name (two or more strings connected by dots, with no spaces). For example, use common.name instead of common name. The string is not required to be an actual domain name. It simply needs to be formatted like one. |
| Email Address<br>*string* | (Optional) Specify your email address, in up to 80 alphanumeric characters with no spaces. |
| Unstructured Name<br>*string* | (Optional) Specify any name, in up to 80 alphanumeric characters with no spaces. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** To use this command, you must already have generated a public-private encryption key pair with the **crypto generate key** command.

**Examples:** To request an administrative certificate from a certificate authority, type the following command:

```
DWS-1008# crypto generate self-signed admin
Country Name:
State Name:
Locality Name:
Organizational Name:
Organizational Unit:
Common Name:
Email Address: m1@example.com
Unstructured Name:
```

**See Also:**
- crypto certificate
- crypto generate key


Download from Www.Somanuals.com. All Manuals Search And Download.

# crypto otp

Sets a one-time password (OTP) for use with the **crypto pkcs12** command.

**Syntax: crypto otp {admin | eap | web}** *one-time-password*

**admin** Creates a one-time password for installing a PKCS#12 object file for an administrative certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the switch to Web View.

**eap** Creates a one-time password for installing a PKCS#12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the switch to 802.1X supplicants (clients).

**web** Creates a one-time password for installing a PKCS#12 object file for a WebAAA certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the switch to WebAAA clients.

*one-time-password* Password of at least 1 alphanumeric character, with no spaces, for clients other than Microsoft Windows clients. The password must be the same as the password protecting the PKCS#12 object file.

**Note:** On a switch that handles communications to and from Microsoft Windows clients, use a one-time password of 31characters or fewer.

The following characters cannot be used as part of the one-time password of a PKCS#12 file:
- Quotation marks (“”)
- Question mark (?)
- Ampersand (&)

**Defaults:** None.

**Access:** Enabled.

**Usage:** The password allows the public-private key pair and certificate to be installed together from the same PKCS#12 object file. MSS erases the one-time password after processing the cryptopkcs12 command or when you reboot the switch.

D-Link recommends that you create a password that is memorable to you but is not subject to easy guesses or a dictionary attack. For best results, create a password of alphanumeric uppercase and lowercase characters.

**Examples:** The following command creates the one-time password hap9iN#ss for installing an EAP certificate and key pair:

```
DWS-1008# crypto generate otp eap hap9iN#ss
OTP set
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# crypto pkcs12

Unpacks a PKCS#12 object file into the certificate and key storage area on the switch. This object file contains a public-private key pair, a switch certificate signed by a certificate authority, and the certificate authority's certificate.

**Syntax: crypto pkcs12 {admin | eap | web}** *file-location-url*

| | |
|---|---|
| **admin** | Unpacks a PKCS#12 object file for an administrative certificate and key pair—and optionally the certificate authority's own certificate—for authenticating the switch to Web View. |
| **eap** | Unpacks a PKCS#12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—for authenticating the switch to 802.1X supplicants (clients). |
| **web** | Unpacks a PKCS#12 object file for a WebAAA certificate and key pair—and optionally the certificate authority's own certificate—for authenticating the switch to WebAAA clients. |
| *file-location-url* | Location of the PKCS#12 object file to be installed. Specify a location of between 1 and 128 alphanumeric characters, with no spaces. |

**Defaults:** The password you enter with the **crypto otp** command must be the same as the one protecting the PKCS#12 file.

**Access:** Enabled.

**Usage:** To use this command, you must have already created a one-time password with the **crypto otp** command.

You must also have the PKCS#12 object file available. You can download a PKCS#12 object file via TFTP from a remote location to the local nonvolatile storage system on the switch.

**Examples:** The following commands copy a PKCS#12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—from a TFTP server to nonvolatile storage on the switch, create the one-time password hap9iN#ss, and unpack the PKCS#12 file:

```
DWS-1008# copy tftp://192.168.253.1/2048full.p12 2048full.p12
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]

DWS-1008# crypto otp eap hap9iN#ss
OTP set

DWS-1008# crypto pkcs12 eap 2048full.p12
Unwrapped from PKCS12 file:
        keypair
        device certificate
        CA certificate
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# show crypto ca-certificate

Displays information about the certificate authority's PEM-encoded PKCS#7 certificate.

**Syntax: show crypto ca-certificate {admin | eap | web}**

**admin** Displays information about the certificate authority's certificate that signed the administrative certificate for the switch. The administrative certificate authenticates the switch to Web View.

**eap** Displays information about the certificate authority's certificate that signed the Extensible Authentication Protocol (EAP) certificate for the switch. The EAP certificate authenticates the DWS to 802.1X supplicants (clients).

**web** Displays information about the certificate authority's certificate that signed the WebAAA certificate for the switch. The WebAAA certificate authenticates the switch to WebAAA clients.

**Defaults:** None.

**Access:** Enabled.

**Examples:** To display information about the certificate of a certificate authority, type the following command:

DWS-1008# **show crypto ca-certificate**

The table below describes the fields in the display.

| Fields | Description |
|---|---|
| Version | Version of the X.509 certificate. |
| Serial Number | A unique identifier for the certificate or signature. |
| Subject | Name of the certificate owner. |
| Signature Algorithm | Algorithm that created the signature, such as RSA MD5 or RSA SHA. |
| Issuer | Certificate authority that issued the certificate or signature. |
| Validity | Time period for which the certificate is valid. |

**See Also:**
- crypto ca-certificate
- show crypto certificate


Download from Www.Somanuals.com. All Manuals Search And Download.

# show crypto certificate

Displays information about one of the cryptographic certificates installed on the switch.

**Syntax: show crypto certificate {admin | eap | web}**

| | |
|---|---|
| **admin** | Displays information about the administrative certificate that authenticates the switch to Web View. |
| **eap** | Displays information about the EAP certificate that authenticates the switch to 802.1X supplicants (clients). |
| **web** | Displays information about the WebAAA certificate that authenticates the switch to WebAAA clients. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** You must have generated a self-signed certificate or obtained a certificate from a certificate authority before displaying information about the certificate.

**Examples:** To display information about a cryptographic certificate, type the following command:

DWS-1008# **show crypto certificate eap**

The table below describes the fields in the display.

## Crypto Certificate Output

| Fields | Description |
|---|---|
| Version | Version of the X.509 certificate. |
| Serial Number | A unique identifier for the certificate or signature. |
| Subject | Name of the certificate owner. |
| Signature Algorithm | Algorithm that created the signature, such as RSA MD5 or RSA SHA. |
| Issuer | Certificate authority that issued the certificate or signature. |
| Validity | Time period for which the certificate is valid. |

**See Also:**
- crypto generate self-signed
- show crypto ca-certificate


Download from Www.Somanuals.com. All Manuals Search And Download.

# show crypto key domain

Displays the checksum (also called a fingerprint) of the public key used to authenticate management traffic between switches.

**Syntax: show crypto key domain**

**Defaults:** None.

**Access:** Enabled.

**Examples:** To display the fingerprint for switch-switch security, type the following command:

```
DWS-1008# show crypto key domain
Domain public key:
e6:43:91:e2:b3:53:ed:46:76:5f:f0:96:3a:3b:86:d3
```

**See Also:**
- crypto generate key

# show crypto key ssh

Displays SSH authentication key information. This command displays the checksum (also called a fingerprint) of the public key. When you connect to the switch with an SSH client, you can compare the SSH key checksum displayed by the switch with the one displayed by the client to verify that you really are connected to the switch and not another device. Generally, SSH clients remember the encryption key after the first connection, so you need to check the key only once.

**Syntax: show show crypto key ssh**

**Defaults:** None.

**Access:** Enabled.

**Examples:** To display SSH key information, type the following command:

```
DWS-1008# show crypto key ssh
ec:6f:56:7f:d1:fd:c0:28:93:ae:a4:f9:7c:f5:13:04
```

**See Also:**
- crypto generate key


Download from Www.Somanuals.com. All Manuals Search And Download.

# RADIUS and Server Groups Commands

Use RADIUS commands to set up communication between a switch and groups of up to four RADIUS servers for remote authentication, authorization, and accounting (AAA) of administrators and network users. This chapter presents RADIUS commands alphabetically. Use the following table to locate commands in this chapter based on their uses.


| | |
|---|---|
| **RADIUS Client** | set radius client system-ip on page 234<br>clear radius client system-ip on page 229 |
| **RADIUS Servers** | set radius on page 232<br>set radius server on page 236<br>clear radius on page 228<br>clear radius server on page 231 |
| **Server Groups** | set server group on page 238<br>set server group load-balance on page 239<br>clear server group on page 231 |
| **RADIUS Proxy** | set radius proxy client on page 234<br>set radius proxy port on page 235<br>clear radius proxy client on page 230<br>clear radius proxy port on page 230 |


(For information about RADIUS attributes, see the RADIUS appendix in the D-Link Mobility System Software Configuration Guide.)



Download from Www.Somanuals.com. All Manuals Search And Download.

# clear radius

Resets parameters that were globally configured for RADIUS servers to their default values.

**Syntax: clear radius {deadtime | key | retransmit | timeout}**

| | |
|---|---|
| **deadtime** | Number of minutes to wait after declaring an unresponsive RADIUS server unavailable before retrying the RADIUS server. |
| **key** | Password (shared secret key) used to authenticate to the RADIUS server. |
| **retransmit** | Number of transmission attempts made before declaring an unresponsive RADIUS server unavailable. |
| **timeout** | Number of seconds to wait for the RADIUS server to respond before retransmitting. |

**Defaults:** Global RADIUS parameters have the following default values:

- **deadtime**—0 (zero) minutes (The switch does not designate unresponsive RADIUS servers as unavailable.)
- **key**—No key
- **retransmit**—3 (the total number of attempts, including the first attempt)
- **timeout**—5 seconds

**Access:** Enabled.

**Usage:** To override the globally set values on a particular RADIUS server, use the **set radius server** command.

**Examples:** To reset all global RADIUS parameters to their factory defaults, type the following commands:

```
DWS-1008# clear radius deadtime
success: change accepted.

DWS-1008# clear radius key
success: change accepted.

DWS-1008# clear radius retransmit
success: change accepted.

DWS-1008# clear radius timeout
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear radius client system-ip

Removes the switch's system IP address from use as the permanent source address in RADIUS client requests from the switch to its RADIUS server(s).

**Syntax: clear radius client system-ip**

| | |
|---|---|
| **deadtime** | Number of minutes to wait after declaring an unresponsive RADIUS server unavailable before retrying the RADIUS server. |
| **key** | Password (shared secret key) used to authenticate to the RADIUS server. |
| **retransmit** | Number of transmission attempts made before declaring an unresponsive RADIUS server unavailable. |
| **timeout** | Number of seconds to wait for the RADIUS server to respond before retransmitting. |

**Defaults:** None

**Access:** Enabled.

**Usage:** The **clear radius client system-ip** command causes the switch to use the IP address of the interface through which it sends a RADIUS client request as the source IP address. The switch selects a source interface address based on information in its routing table as the source address for RADIUS packets leaving the switch.

**Examples:** To clear the system IP address as the permanent source address for RADIUS client requests, type the following command:

```
DWS-1008# clear radius client system-ip
success: change accepted.
```

**See Also:**
- set radius client system-ip
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear radius proxy client

Removes RADIUS proxy client entries for third-party APs.

**Syntax: clear radius proxy client all**

**Defaults:** None

**Access:** Enabled.

**Examples:** The following command clears all RADIUS proxy client entries from the switch:

```
DWS-1008# clear radius proxy client all
success: change accepted.
```

**See Also:**
- set radius proxy client

# clear radius proxy port

Removes RADIUS proxy ports configured for third-party APs.

**Syntax: clear radius proxy port all**

**Defaults:** None

**Access:** Enabled.

**Examples:** The following command clears all RADIUS proxy port entries from the switch:

```
DWS-1008# clear radius proxy port all
success: change accepted.
```

**See Also:**
- set radius proxy port


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear radius server

Removes the named RADIUS server from the switch configuration.

**Syntax: clear radius server** *server-name*

*server-name* Name of a RADIUS server configured to perform remote AAA services for the switch.

**Defaults:** None

**Access:** Enabled.

**Examples:** The following command removes the RADIUS server rs42 from a list of remote AAA servers:

```
DWS-1008# clear radius server rs42
success: change accepted.
```

**See Also:**
- set radius server
- show aaa

# clear server group

Removes a RADIUS server group from the configuration, or disables load balancing for the group.

**Syntax: clear server group** *group-name* **[load-balance]**

*group-name* Name of a RADIUS server group configured to perform remote AAA services for switches.

**load-balance** Ability of group members to share demand for services among servers.

**Defaults:** None

**Access:** Enabled.

**Usage:** Deleting a server group removes the server group from the configuration. However, the members of the server group remain.

**Examples:** To remove the server group sg-77 type the following command:

```
DWS-1008# clear server group sg-77
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

To disable load balancing in a server group *shorebirds*, type the following command:

```
DWS-1008# set server group shorebirds load-balance disable
success: change accepted.
```

**See Also:**
- set server group

# set radius

Configures global defaults for RADIUS servers that do not explicitly set these values themselves. By default, the switch automatically sets all these values except the password (key).

**Syntax: set radius {deadtime** *minutes* **| encrypted-key** *string* **| key** *string* **| retransmit** *number* **| timeout** *seconds***}**

| | |
|---|---|
| **deadtime** *minutes* | Number of minutes the switch waits after declaring an unresponsive RADIUS server unavailable before retrying the RADIUS server. You can specify from 0 to 1440 minutes. |
| **encrypted-key** *string* | Password (shared secret key) used to authenticate to the RADIUS server, entered in its encrypted form. You must provide the same encrypted password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs. MSS does not encrypt the string you enter, and instead displays the string in **show config** and **show aaa** output exactly as you entered it.<br><br>**Note:** Use this option only if you are entering the key in its encrypted form. To enter the key in unencrypted form, use the **key** *string* option instead. |
| **key** *string* | Password (shared secret key) used to authenticate to the RADIUS server, entered in its unencrypted form. You must provide the same password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs. MSS encrypts the displayed form of the string in **show config** and **show aaa** output. |
| **retransmit** *number* | Number of transmission attempts the switch makes before declaring an unresponsive RADIUS server unavailable. You can specify from 1 to100 retries. |
| **timeout** *seconds* | Number of seconds the switch waits for the RADIUS server to respond before retransmitting. You can specify from 1 to 65,535. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** Global RADIUS parameters have the following default values:

- **deadtime**—0 (zero) minutes (The switch does not designate unresponsive RADIUS servers as unavailable.)
- **encrypted-key**—No key
- **key**—No key
- **retransmit**—3 (the total number of attempts, including the first attempt)
- **timeout**—5 seconds

**Access:** Enabled.

**Usage:** You can specify only one parameter per command line.

**Examples:** The following commands sets the dead time to 5 minutes, the RADIUS key to goody, the number of retransmissions to 1, and the timeout to 21 seconds on all RADIUS servers connected to the switch:

```
DWS-1008# set radius deadtime 5
success: change accepted.

DWS-1008# set radius key goody
success: change accepted.

DWS-1008# set radius retransmit 1
success: change accepted.

DWS-1008# set radius timeout 21
success: change accepted.
```

**See Also:**
- clear radius server
- set radius server
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# set radius client system-ip

Causes all RADIUS requests to be sourced from the IP address specified by the set system ip-address command, providing a permanent source IP address for RADIUS packets sent from the switch.

**Syntax: set radius client system-ip**

**Defaults:** None. If you do not use this command, RADIUS packets leaving the switch have the source IP address of the outbound interface, which can change as routing conditions change.

**Access:** Enabled.

**Usage:** The switch system IP address must be set before you use this command.

**Examples:** The following command sets the switch system IP address as the address of the RADIUS client:

```
DWS-1008# set radius client system-ip
success: change accepted.
```

**See Also:**
- clear radius client system-ip
- set system ip-address

# set radius proxy client

Adds a RADIUS proxy entry for a third-party AP. The proxy entry specifies the IP address of the AP and the UDP ports on which the switch listens for RADIUS traffic from the AP.

**Syntax: set radius proxy client address** *ip-address* **[acct-port** *acct-udp-port-number***] [port** *udp-port-number***] key** *string*

| | |
|---|---|
| **address** *ip-address* | IP address of the third-party AP. Enter the address in dotted decimal notation. |
| **port** *udp-port-number* | UDP port on which the switch listens for RADIUS access-requests from the AP. |
| **acct-port** *acct-udp-port-number* | UDP port on which the switch listens for RADIUS stop-accounting records from the AP. |
| **key** *string* | Password (shared secret key) the switch uses to authenticate and encrypt RADIUS communication. |

**Defaults:** The default UDP port number for access-requests is 1812. The default UDP port number for stop-accounting records is 1813.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Access:** Enabled.

**Usage:** AAA for third-party AP users has additional configuration requirements.

**Examples:** The following command configures a RADIUS proxy entry for a third-party AP RADIUS client at 10.20.20.9, sending RADIUS traffic to the default UDP ports 1812 and 1813 on the switch:

```
DWS-1008# set radius proxy client address 10.20.20.9 key radkey1
success: change accepted.
```

**See Also:**
- clear radius proxy client
- set authentication proxy
- set radius proxy port

# set radius proxy port

Configures the switch port connected to a third-party AP as a RADIUS proxy for the SSID supported by the AP.

**Syntax: set radius proxy port** *port-list* **[tag** *tag-value***] ssid** *ssid-name*

| | |
|---|---|
| **port** *port-list* | Switch port(s) connected to the third-party AP. |
| **tag** *tag-value* | 802.1Q tag value in packets sent by the third-party AP for the SSID. |
| **ssid** *ssid-name* | SSID supported by the third-party AP. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** AAA for third-party AP users has additional configuration requirements.

Enter a separate command for each SSID, and its tag value, you want the switch to support.

**Examples:** The following command maps SSID mycorp to packets received on port 3 or 4, using 802.1Q tag value 104:

```
DWS-1008# set radius proxy port 3-4 tag 104 ssid mycorp
success: change accepted.
```

**See Also:**
- clear radius proxy port
- set authentication proxy
- set radius proxy client


Download from Www.Somanuals.com. All Manuals Search And Download.

# set radius server

Configures RADIUS servers and their parameters. By default, the switch automatically sets all these values except the password (key).

**Syntax: set radius server** *server-name* **[address** *ip-address***] [auth-port** *port-number***] [acct-port** *port-number***] [timeout** *seconds***] [retransmit** *number***] [deadtime** *minutes***] [[key** *string***] | [encrypted-key** *string***]] [author-password** *password***]**

| | |
|---|---|
| *server-name* | Unique name for this RADIUS server. Enter an alphanumeric string of up to 32 characters, with no blanks. |
| **address** *ip-address* | IP address of the RADIUS server. Enter the address in dotted decimal notation. |
| **auth-port** *port-number* | UDP port that the switch uses for authentication and authorization. |
| **acct-port** port-number | UDP port that the switch uses for accounting. |
| **timeout** *seconds* | Number of seconds the switch waits for the RADIUS server to respond before retransmitting. You can specify from 1 to 65,535 seconds. |
| **retransmit** *number* | Number of transmission attempts made before declaring an unresponsive RADIUS server unavailable. You can specify from 1 to 100 retries. |
| **deadtime** *minutes* | Number of minutes the switch waits after declaring an unresponsive RADIUS server unavailable before retrying that RADIUS server. Specify between 0 (zero) and 1440 minutes (24 hours). A zero value causes the switch to identify unresponsive servers as available. |
| **key** *string* \| **encrypted-key** *string* | Password (shared secret key) the switch uses to authenticate to RADIUS servers. You must provide the same password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs.<br>• Use the **key** option to enter the string in its unencrypted form. MSS encrypts the displayed form of the string in **show config** and **show aaa** output.<br>• To enter the string in its encrypted form instead, use the **encrypted-key** option. MSS does not encrypt the string you enter, and instead displays the string exactly as you enter it. |
| **author-password** *password* | Number of minutes the switch waits after declaring an unresponsive RADIUS server unavailable before retrying that RADIUS server. Specify between 0 (zero) and 1440 minutes (24 hours). A zero value causes the switch to identify unresponsive servers as available. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** Default values are listed below:

- **auth-port**—UDP port1812
- **acct-port**—UDP port1813
- **timeout**—5 seconds
- **retransmit**—3 (the total number of attempts, including the first attempt)
- **deadtime**—0 (zero) minutes (The switch does not designate unresponsive RADIUS servers as unavailable.)
- **key**—No key
- **encrypted-key**—No key
- **author-password**—trapeze

**Access:** Enabled.

**Usage:** or a given RADIUS server, the first instance of this command must set both the server name and the IP address and can include any or all of the other optional parameters. Subsequent instances of this command can be used to set optional parameters for a given RADIUS server.

To configure the server as a remote authenticator for the switch, you must add it to a server group with the **set server group** command.

Do not use the same name for a RADIUS server and a RADIUS server group.

**Examples:** To set a RADIUS server named RS42 with IP address 198.162.1.1 to use the default accounting and authorization ports with a timeout interval of 30 seconds, two transmit attempts, 5 minutes of dead time, a key string of keys4u, and the default authorization password of *dlink*, type the following command:

```
DWS-1008# set radius server RS42 address 198.162.1.1 timeout 30 retransmit 2
deadtime 5 key keys4U
```

**See Also:**
- set authentication admin
- set authentication console
- set authentication dot1x
- set authentication mac
- set authentication web
- set radius
- set server group
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# set server group

Configures a group of one to four RADIUS servers.

**Syntax: set server group** *group-name* **members** *server-name1* **[***server-name2***] [***server-name3***] [***server-name4***]**

| | |
|---|---|
| *group-name* | Server group name of up to 32 characters, with no spaces or tabs. |
| **members**<br>*server-name1*<br>*server-name2*<br>*server-name3*<br>*server-name4* | The names of one or more configured RADIUS servers. You can enter up to four server names. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** You must assign all group members simultaneously, as shown in the example. To enable load balancing, use **set server group load-balance enable**.

Do not use the same name for a RADIUS server and a RADIUS server group.

**Examples:** To set server group *shorebirds* with members *heron, egret*, and *sandpiper*, type the following command:

```
DWS-1008# set server group shorebirds members heron egret sandpiper
success: change accepted.
```

**See Also:**
- clear server group
- set server group load-balance
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# set server group load-balance

Enables or disables load balancing among the RADIUS servers in a server group.

**Syntax: set server group** *group-name* **load-balance {enable | disable}**

| | |
|---|---|
| *group-name* | Server group name of up to 32 characters. |
| **load-balance enable \| disable** | Enables or disables load balancing of authentication requests among the servers in the group. |

**Defaults:** Load balancing is disabled by default.

**Access:** Enabled.

**Usage:** You can optionally enable load balancing after assigning the server group members. If you configure load balancing, MSS sends each AAA request to a separate server, starting with the first one on the list and skipping unresponsive servers. If no server in the group responds, MSS moves to the next method configured with **set authentication** and **set accounting**.

In contrast, if load balancing is not configured, MSS always begins with the first server in the list and sends unfulfilled requests to each subsequent server in the group before moving on to the next configured AAA method.

**Examples:** To enable load balancing between the members of server group *shorebirds*, type the following command:

```
DWS-1008# set server group shorebirds load-balance enable
success: change accepted.
```

To disable load balancing between *shorebirds* server group members, type the following command:

```
DWS-1008# set server group shorebirds load-balance disable
success: change accepted.
```

**See Also:**
- clear server group
- clear radius server
- set server group
- show aaa


Download from Www.Somanuals.com. All Manuals Search And Download.

# 802.1X Management Commands

Use 802. IEEE X management commands to modify the default settings for IEEE 802.1X sessions on a DWS-1008 switch. For best results, change the settings only if you are aware of a problem with the switch's 802.1X performance.

This chapter presents 802.1X commands alphabetically. Use the following table to locate commands in this chapter based on their use.

**Caution:** 802.1X parameter settings are global for all SSIDs configured on the switch.

| | |
|---|---|
| **Wired Authentication Port Control** | set dot1x port-control on page 248<br>clear dot1x port-control on page 242<br>set dot1x authcontrol on page 245 |
| **Keys** | set dot1x key-tx on page 247<br>set dot1x tx-period on page 251<br>clear dot1x tx-period on page 245<br>set dot1x wep-rekey on page 252<br>set dot1x wep-rekey-period on page 252 |
| **Bonded Authentication** | clear dot1x bonded-period on page 241<br>set dot1x bonded-period on page 246 |
| **Reauthentication** | set dot1x reauth-max on page 249<br>clear dot1x reauth-max on page 243<br>set dot1x reauth-period on page 250<br>clear dot1x reauth-period on page 243 |
| **Retransmission** | set dot1x quiet-period on page 249<br>clear dot1x quiet-period on page 242<br>set dot1x timeout auth-server on page 250<br>clear dot1x timeout auth-server on page 244<br>set dot1x timeout supplicant on page 251<br>clear dot1x timeout supplicant on page 244 |


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear dot1x bonded-period

Resets the Bonded Auth period to its default value.

**Syntax: clear dot1x max-req**

**Defaults:** The default bonded authentication period is 0 seconds.

**Access:** Enabled.

**Examples:** To reset the Bonded period to its default, type the following command:

```
DWS-1008# clear dot1x bonded-period
success: change accepted
```

**See Also:**
- set dot1x bonded-period
- show dot1x

# clear dot1x max-req

Resets to the default setting the number of Extensible Authentication Protocol (EAP) requests that the switch retransmits to a supplicant (client).

**Syntax: clear dot1x max-req**

**Defaults:** The default number is 20.

**Access:** Enabled.

**Examples:** To reset the number of 802.1X requests the switch can send to the default setting, type the following command:

```
DWS-1008# clear dot1x max-req
success: change accepted
```

**See Also:**
- set dot1x max-req
- show dot1x


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear dot1x port-control

Resets all wired authentication ports on the switch to default 802.1X authentication.

**Syntax: clear dot1x port-control**

**Defaults:** By default, all wired authentication ports are set to auto and they process authentication requests as determined by the **set authentication dot1X** command.

**Access:** Enabled.

**Usage:** This command is overridden by the **set dot1x authcontrol** command. The **clear dot1x port-control** command returns port control to the method configured. This command applies only to wired authentication ports.

**Examples:** Type the following command to reset the wired authentication port control:

```
DWS-1008# clear dot1x port-control
success: change accepted
```

**See Also:**
- set dot1x port-control
- show dot1x

# clear dot1x quiet-period

Resets the quiet period after a failed authentication to the default setting.

**Syntax: clear dot1x quiet-period**

**Defaults:** The default is 60 seconds.

**Access:** Enabled.

**Examples:** Type the following command to reset the 802.1X quiet period to the default:

```
DWS-1008# clear dot1x quiet-period
success: change accepted
```

**See Also:**
- set dot1x quiet-period
- show dot1x


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear dot1x reauth-max

Resets the maximum number of reauthorization attempts to the default setting.

**Syntax: clear dot1x reauth-max**

**Defaults:** The default is 2 attempts.

**Access:** Enabled.

**Examples:** Type the following command to reset the maximum number of reauthorization attempts to the default:

```
DWS-1008# clear dot1x reauth-max
success: change accepted
```

**See Also:**
- set dot1x reauth-max
- show dot1x

# clear dot1x reauth-period

Resets the time period that must elapse before a reauthentication attempt, to the default time period.

**Syntax: clear dot1x reauth-period**

**Defaults:** The default is 3600 seconds (1hour).

**Access:** Enabled.

**Examples:** Type the following command to reset the default reauthentication time period:

```
DWS-1008# clear dot1x reauth-period
success: change accepted
```

**See Also:**
- set dot1x reauth-period
- show dot1x


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear dot1x timeout auth-server

Resets to the default setting the number of seconds that must elapse before the switch times out a request to a RADIUS server.

**Syntax: clear dot1x reauth-period**

**Defaults:** The default is 30 seconds.

**Access:** Enabled.

**Examples:** To reset the default timeout for requests to an authentication server, type the following command:

```
DWS-1008# clear dot1x timeout auth-server
success: change accepted
```

**See Also:**
- set dot1x timeout auth-server
- show dot1x

# clear dot1x timeout supplicant

Resets to the default setting the number of seconds that must elapse before the switch times out an authentication session with a supplicant (client).

**Syntax: clear dot1x timeout supplicant**

**Defaults:** The default for the authentication timeout sessions is 30 seconds.

**Access:** Enabled.

**Examples:** Type the following command to reset the timeout period for an authentication session:

```
DWS-1008# clear dot1x timeout supplicant
success: change accepted
```

**See Also:**
- set dot1x timeout supplicant
- show dot1x


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear dot1x tx-period

Resets to the default setting the number of seconds that must elapse before the switch retransmits an EAP over LAN (EAPoL) packet.

**Syntax: clear dot1x tx-period**

**Defaults:** The default is 5 seconds.

**Access:** Enabled.

**Examples:** Type the following command to reset the EAPoL retransmission time:

```
DWS-1008# clear dot1x tx-period
success: change accepted
```

**See Also:**
- set dot1x tx-period
- show dot1x

# set dot1x authcontrol

Provides a global override mechanism for 802.1X authentication configuration on wired authentication ports.

**Syntax: set dot1x authcontrol {enable | disable}**

| | |
|---|---|
| **enable** | Allows all wired authentication ports running 802.1X to use the authentication specified per port by the **set dot1X port-control** command. |
| **disable** | Forces all wired authentication ports running 802.1X to unconditionally accept all 802.1X authentication attempts with an EAP Success message (ForceAuth). |

**Defaults:** By default, authentication control for individual wired authentication is enabled.

**Access:** Enabled.

**Usage:** This command applies only to wired authentication ports.

**Examples:** To enable per-port 802.1X authentication on wired authentication ports, type the following command:

```
DWS-1008# set dot1x authcontrol enable
success: dot1x authcontrol enabled.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set dot1x bonded-period

Changes the Bonded Auth™ (bonded authentication) period. The *Bonded Auth period* is the number of seconds MSS allows a Bonded Auth user to reauthenticate.

**Syntax: set dot1x bonded-period** *seconds*

| | |
|---|---|
| *seconds* | Number of seconds MSS retains session information for an authenticated machine while waiting for a client to (re)authenticate on the same machine. You can change the bonded authentication period to a value from 1 to 300 seconds. |

**Defaults:** The default bonded period is 0 seconds, which disables the feature.

**Access:** Enabled.

**Usage:** Normally, the Bonded Auth period needs to be set only if the network has Bonded Auth clients that use dynamic WEP, or use WEP-40 or WEP-104 encryption with WPA or RSN. These clients can be affected by the 802.1X reauthentication parameter or the RADIUS Session-Timeout parameter.

D-Link recommends that you try 60 seconds, and change the period to a longer value only if clients are unable to authenticate within 60 seconds.

The bonded authentication period applies only to 802.1X authentication rules that contain the **bonded** option.

**Examples:** To set the bonded authentication period to 60 seconds, type the following command:

```
DWS-1008# set dot1x bonded-period 60
success: change accepted.
```

**See Also:**
- clear dot1x bonded-period
- show dot1x


Download from Www.Somanuals.com. All Manuals Search And Download.

# set dot1x key-tx

Enables or disables the transmission of encryption key information to the supplicant (client) in EAP over LAN (EAPoL) key messages, after authentication is successful.

**Syntax: set dot1x key-tx {enable | disable}**

| | |
|---|---|
| **enable** | Enables transmission of encryption key information to clients. |
| **disable** | Disables transmission of encryption key information to clients. |

**Defaults:** Key transmission is enabled by default.

**Access:** Enabled.

**Examples:** Type the following command to enable key transmission:

```
DWS-1008# set dot1x key-tx enable
success: dot1x key transmission enabled.
```

**See Also:**
- show dot1x

# set dot1x max-req

Sets the maximum number of times the switch retransmits an EAP request to a supplicant (client) before ending the authentication session.

**Syntax: set dot1x max-req** *number-of-retransmissions*

| | |
|---|---|
| *number-of-retransmissions* | Specify a value between 0 and 10. |

**Defaults:** The default number of EAP retransmissions is 2.

**Access:** Enabled.

**Usage:** To support SSIDs that have both 802.1X and static WEP clients, MSS sends a maximum of two ID requests, even if this parameter is set to a higher value. Setting the parameter to a higher value does affect all other types of EAP messages.

**Examples:** Type the following command to set the maximum number of EAP request retransmissions to three attempts:

```
DWS-1008# set dot1x max-req 3
success: dot1x max request set to 3.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

**See Also:**
- clear dot1x max-req
- show dot1x

# set dot1x port-control

Determines the 802.1X authentication behavior on individual wired authentication ports or groups of ports.

**Syntax: set dot1x port-control {forceauth | forceunauth | auto}** *port-list*

| | |
|---|---|
| **forceauth** | Forces the specified wired authentication port(s) to *unconditionally authorize* all 802.1X authentication attempts, with an EAP success message. |
| **forceunauth** | Forces the specified wired authentication port(s) to *unconditionally reject* all 802.1X authentication attempts with an EAP failure message. |
| **auto** | Allows the specified wired authentication ports to process 802.1X authentication normally as determined for the user by the **set authentication dot1X** command. |
| *port-list* | One or more wired authentication ports for which to set 802.1X port control. |

**Defaults:** By default, wired authentication ports are set to auto.

**Access:** Enabled.

**Usage:** This command affects only wired authentication ports.

**Examples:** The following command forces port 6 to unconditionally accept all 802.1X authentication attempts:

```
DWS-1008# set dot1x port-control forceauth 6
success: authcontrol for 19 is set to FORCE-AUTH.
```

**See Also:**
- show port status
- show dot1x


Download from Www.Somanuals.com. All Manuals Search And Download.

# set dot1x quiet-period

Sets the number of seconds a switch remains quiet and does not respond to a supplicant after a failed authentication.

**Syntax: set dot1x quiet-period** *seconds*

*seconds* Specify a value between 0 and 65,535.

**Defaults:** The default is 60 seconds.

**Access:** Enabled.

**Examples:** Type the following command to set the quiet period to 90 seconds:

```
DWS-1008# set dot1x reauth enable
success: dot1x reauthentication enabled.
```

**See Also:**
- set dot1x reauth-max
- set dot1x reauth-period
- show dot1x

# set dot1x reauth-max

Sets the number of reauthentication attempts that the switch makes before the supplicant (client) becomes unauthorized.

**Syntax: set dot1x reauth-max** *number-of-attempts*

*number-of-attempts* Specify a value between 1 and 10.

**Defaults:** The default number of reauthentication attempts is 2.

**Access:** Enabled.

**Usage:** If the number of reauthentications for a wired authentication client is greater than the maximum number of reauthentications allowed, MSS sends an EAP failure packet to the client and removes the client from the network. However, MSS does not remove a wireless client from the network under these circumstances.

**Examples:** Type the following command to set the number of authentication attempts to 8:

```
DWS-1008# set dot1x reauth-max 8
success: dot1x max reauth set to 8.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set dot1x reauth-period

Sets the number of seconds that must elapse before the switch attempts reauthentication.

**Syntax: set dot1x reauth-period** *seconds*

*seconds* Specify a value between 60 (1 minute) and 1,641,600 (19 days).

**Defaults:** The default is 3600 seconds (1 hour).

**Access:** Enabled.

**Usage:** You also can use the RADIUS session-timeout attribute to set the reauthentication timeout for a specific client. In this case, MSS uses the timeout that has the lower value. If the session-timeout is set to fewer seconds than the global reauthentication timeout, MSS uses the session-timeout for the client. However, if the global reauthentication timeout is shorter than the session-timeout, MSS uses the global timeout instead.

**Examples:** Type the following command to set the number of seconds to 100 before reauthentication is attempted:

```
DWS-1008# set dot1x reauth-period 100
success: dot1x auth-server timeout set to 100.
```

**See Also:**
- clear dot1x reauth-period
- show dot1x

# set dot1x timeout auth-server

Sets the number of seconds that must elapse before the switch times out a request to a RADIUS authentication server.

**Syntax: set dot1x timeout auth-server** *seconds*

*seconds* Specify a value between 1 and 65,535.

**Defaults:** The default is 30 seconds.

**Access:** Enabled.

**Examples:** Type the following command to set the authentication server timeout to 60 seconds:

```
DWS-1008# set dot1x timeout auth-server 60
success: dot1x auth-server timeout set to 60.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set dot1x timeout supplicant

Sets the number of seconds that must elapse before the switch times out an authentication session with a supplicant (client).

**Syntax: set dot1x timeout supplicant** *seconds*

| | |
|---|---|
| *seconds* | Specify a value between 1 and 65,535. |

**Defaults:** The default is 30 seconds.

**Access:** Enabled.

**Examples:** Type the following command to set the number of seconds for authentication session timeout to 300:

```
DWS-1008# set dot1x timeout supplicant 300
success: dot1x supplicant timeout set to 300.
```

**See Also:**
- clear dot1x timeout auth-server
- show dot1x

# set dot1x tx-period

Sets the number of seconds that must elapse before the switch retransmits an EAPoL packet.

**Syntax: set dot1x tx-period** *seconds*

| | |
|---|---|
| *seconds* | Specify a value between 1 and 65,535. |

**Defaults:** The default is 5 seconds.

**Access:** Enabled.

**Examples:** Type the following command to set the number of seconds before the switch retransmits an EAPoL packet to 300:

```
DWS-1008# set dot1x tx-period 300
success: dot1x tx-period set to 300.
```

**See Also:**
- clear dot1x tx-period
- show dot1x


Download from Www.Somanuals.com. All Manuals Search And Download.

# set dot1x wep-rekey

Enables or disables Wired Equivalency Privacy (WEP) rekeying for broadcast and multicast encryption keys.

**Syntax: set dot1X wep-rekey {enable | disable}**

| | |
|---|---|
| **enable** | Causes the broadcast and multicast keys for WEP to be rotated at an interval set by the set dot1x wep-rekey-period for each radio, associated VLAN, and encryption type. The switch generates the new broadcast and multicast keys and pushes the keys to the clients via EAPoL key messages. |
| **disable** | WEP broadcast and multicast keys are never rotated. |

**Defaults:** WEP key rotation is enabled, by default.

**Access:** Enabled.

**Usage:** Reauthentication is not required for WEP key rotation to take place. Broadcast and multicast keys are always rotated at the same time, so all members of a given radio, VLAN, or encryption type receive the new keys at the same time.

**Examples:** Type the following command to disable WEP key rotation:

```
DWS-1008# set dot1x wep-rekey disable
success: wep rekeying disabled
```

**See Also:**
- set dot1x wep-rekey-period
- show dot1x

# set dot1x wep-rekey-period

Sets the interval for rotating the WEP broadcast and multicast keys.

**Syntax: set dot1x wep-rekey-period** *seconds*

| | |
|---|---|
| *seconds* | Specify a value between 30 and 1,641,600 (19 days). |

**Defaults:** The default is 1800 seconds (30 minutes).

**Access:** Enabled.

**Examples:** Type the following command to set the WEP-rekey period to 300 seconds:

```
DWS-1008# set dot1x wep-rekey-period 300
success: dot1x wep-rekey-period set to 300
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# show dot1x

Displays 802.1X client information for statistics and configuration settings.

**Syntax: show dot1x {clients | stats | config}**

**clients** Displays information about active 802.1X clients, including client name, MAC address, and state.

**stats** Displays global 802.1X statistics associated with connecting and authenticating.

**config** Displays a summary of the current configuration.

**Defaults:** None.

**Access:** Enabled.

**Examples:** Type the following command to display the 802.1X clients:

```
DWS-1008# show dot1x clients
MAC Address        State          Vlan        Identity
-------------------------------------------------------------------------------------------
00:20:a6:48:01:1f  Connecting     (unknown)
00:05:3c:07:6d:7c  Authenticated  vlan-it     EXAMPLE\jose
00:05:5d:7e:94:83  Authenticated  vlan-eng    EXAMPLE\singh
00:02:2d:86:bd:38  Authenticated  vlan-eng    bard@xmple.com
00:05:5d:7e:97:b4  Authenticated  vlan-eng    EXAMPLE\havel
00:05:5d:7e:98:1a  Authenticated  vlan-eng    EXAMPLE\nash
00:0b:be:a9:dc:4e  Authenticated  vlan-pm     xalik@xmple.com
00:05:5d:7e:96:e3  Authenticated  vlan-eng    EXAMPLE\mishan
00:02:2d:6f:44:77  Authenticated  vlan-eng    EXAMPLE\ethan
00:05:5d:7e:94:89  Authenticated  vlan-eng    EXAMPLE\fmarshall
00:06:80:00:5c:02  Authenticated  vlan-eng    EXAMPLE\bmccarthy
00:02:2d:6a:de:f2  Authenticated  vlan-pm     neailey@xmple.com
00:02:2d:5e:5b:76  Authenticated  vlan-pm     EXAMPLE\tamara
00:02:2d:80:b6:e1  Authenticated  vlan-cs     dmc@xmple.com
00:30:65:16:8d:69  Authenticated  vlan-wep    MAC authenticated
00:02:2d:64:8e:1b  Authenticated  vlan-eng    EXAMPLE\wong
```


Download from Www.Somanuals.com. All Manuals Search And Download.

Type the following command to display the 802.1X clients:

```
DWS-1008# show dot1x config
                  802.1X user policy
                  ----------------------
‘host/bob-laptop.mycorp.com’ on ssid ‘mycorp’ doing PASSTHRU
’bob.mycorp.com’ on ssid ‘mycorp’ doing PASSTHRU (bonded)

802.1X parameter                  setting
----------------------            ----------------------
supplicant timeout                30
auth-server timeout               30
quiet period                      5
transmit period                   5
reauthentication period           3600
maximum requests                  2
key transmission                  enabled
reauthentication                  enabled
authentication control            enabled
WEP rekey period                  1800
WEP rekey                         enabled
Bonded period                     60

port 5, authcontrol: auto, max-sessions: 16
port 6, authcontrol: auto, max-sessions: 1
port 7, authcontrol: auto, max-sessions: 1
port 8, authcontrol: auto, max-sessions: 1
```


Download from Www.Somanuals.com. All Manuals Search And Download.

Type the following command to display 802.1X statistics:

```
DWS-1008# show dot1x stats
802.1X statistic                    value
--------------------                ----------------------
Enters Connecting:                  709
Logoffs While Connecting:           112
Enters Authenticating:              467
Success While Authenticating:       0
Timeouts While Authenticating:      52
Failures While Authenticating:      0
Reauths While Authenticating:       0
Starts While Authenticating:        31
Logoffs While Authenticating:       0
Starts While Authenticated:         85
Logoffs While Authenticated:        1
Bad Packets Received:               0
```

The table below explains the counters in the **show dot1x stats** output.

| Field | Description |
|---|---|
| Enters Connecting | Number of times that the switch state transitions to the CONNECTING state from any other state. |
| Logoffs While Connecting | Number of times that the switch state transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPoL-Logoff message. |
| Enters Authenticating | Number of times that the state wildcard transitions. |
| Success While Authenticating | Number of times the switch state transitions from AUTHENTICATING from AUTHENTICATED, as a result of an EAP-Response/Identity message being received from the supplicant (client). |
| Timeouts While Authenticating | Number of times that the switch state wildcard transitions from AUTHENTICATING to ABORTING. |
| Failures While Authenticating | Number of times that the switch state wildcard transitions from AUTHENTICATION to HELD. |
| Reauths While Authenticating | Number of times that the switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE). |
| Starts While Authenticating | Number of times that the switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of an EAPoL-Start message being received from the Supplicant (client). |
| Logoffs While Authenticating | Number of times that the switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of an EAPoL-logoff message being received from the Supplicant (client). |
| Bad Packets Received | Number of EAPoL packets received that have an invalid version or type. |


Download from Www.Somanuals.com. All Manuals Search And Download.

# Session Management Commands

Use session management commands to display and clear administrative and network user sessions. This chapter presents session management commands alphabetically. Use the following table to locate commands in this chapter based on their use.


| | |
|---|---|
| **Administrative Sessions** | show sessions on page 258<br>clear sessions on page 256 |
| **Network Sessions** | show sessions network on page 260<br>clear sessions network on page 257 |


## clear sessions

Clears all administrative sessions, or clears administrative console or Telnet sessions.

**Syntax: clear sessions {admin | console | telnet[client[*session-id*]]}**

| | |
|---|---|
| **admin** | Clears sessions for all users with administrative access to the switch through a Telnet or SSH connection or a console plugged into the switch. |
| **console** | Clears sessions for all users with administrative access to the switch through a console plugged into the switch. |
| **telnet** | Clears sessions for all users with administrative access to the switch through a Telnet connection. |
| **telnetclient** [*session-id*] | Clears all Telnet client sessions from the CLI to remote devices, or clears an individual session identified by session ID. |

**Defaults:** None.

**Access:** Enabled.

**Examples:** To clear all administrator sessions type the following command:

```
DWS-1008# clear sessions admin
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```

To clear all administrative sessions through the console, type the following command:

```
DWS-1008# clear sessions console
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```



Download from Www.Somanuals.com. All Manuals Search And Download.

To clear all administrative Telnet sessions, type the following command:

```
DWS-1008# clear sessions telnet
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```

To clear Telnet client session 0, type the following command:

```
DWS-1008# clear sessions telnet client 0
```

**See Also:**
• show sessions

# clear sessions network

Clears all network sessions for a specified username or set of usernames, MAC address or set of MAC addresses, virtual LAN (VLAN) or set of VLANs, or session ID.

**Syntax: clear sessions network {user** *user-glob* **| mac-addr** *mac-addr-glob* **| vlan** *vlan-glob* **| session-id** *local-session-id***}**

| | |
|---|---|
| **user** *user-glob* | Clears all network sessions for a single user or set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globs” on page 6.) |
| **mac-addr** *mac-addr-glob* | Clears all network sessions for a MAC address. Specify a MAC address in hexadecimal numbers separated by colons (:), or use the wildcard character (*) to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 7.) |
| **vlan** *vlan-glob* | Clears all network sessions on a single VLAN or a set of VLANs. Specify a VLAN name, use the double-asterisk wildcard character (**) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an at sign (@) or a period (.). (For details, see “VLAN Globs” on page 6.) |
| **session-id** *local-session-id* | Clears the specified 802.1X network session. To find local session IDs, use the **show sessions** command. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** The **clear sessions network** command clears network sessions by deauthenticating and, for wireless clients, disassociating them.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** To clear all sessions for MAC address 00:01:02:03:04:05, type the following command:

```
DWS-1008# clear sessions network mac-addr 00:01:02:03:04:05
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```

To clear session 9, type the following command:

```
DWS-1008# clear sessions network session-id 9
SM Apr 11 19:53:38 DEBUG SM-STATE: localid 9, mac 00:06:25:09:39:5d,
flags 0000012fh, to change state to KILLING
Localid 9, globalid SESSION-9-893249336 moved from ACTIVE to KILLING
(client=00:06:25:09:39:5d)
```

To clear the session of user *Natasha*, type the following command:

```
DWS-1008# clear sessions network user Natasha
```

To clear the sessions of users whose name begins with the characters *Jo*, type the following command:

```
DWS-1008# clear sessions network user Jo*
```

To clear the sessions of all users on VLAN *red*, type the following command:

```
DWS-1008# clear sessions network vlan red
```

**See Also:**
- show sessions
- show sessions network

# show sessions

Displays session information and statistics for all users with administrative access to the switch, or for administrative users with either console or Telnet access.

**Syntax: show sessions {admin | console | telnet [client]}**

| | |
|---|---|
| **admin** | Displays sessions for all users with administrative access to the switch through a Telnet or SSH connection or a console plugged into the switch. |
| **console** | Displays sessions for all users with administrative access to the switch through a console plugged into the switch. |
| **telnet** | Displays sessions for all users with administrative access to the switch through a Telnet connection. |
| **telnet client** | Displays Telnet sessions from the CLI to remote devices. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** All, except for **show sessions telnet client**, which has enabled access.

**Examples:** To view information about sessions of administrative users, type the following command:

```
DWS-1008# clear sessions admin
Tty          Username          Time (s)     Type
-------      --------------------  --------     ----
tty0                           3644         Console
tty2         tech              6            Telnet
tty3         sshadmin          381          SSH

3 admin sessions
```

To view information about console users' sessions, type the following command:

```
DWS-1008# show sessions console
Tty          Username          Time (s)
-------      --------------------  --------
console                        8573

1 console session
```

To view information about Telnet users sessions, type the following command:

```
DWS-1008# show sessions telnet
TTty         Username          Time (s)
-------      --------------------  --------
tty2         sea               7395
```

To view information about Telnet client sessions, type the following command:

```
DWS-1008# show sessions telnet client
Session      Server Address    Server Port    Client Port
--------     --------------    ------------   -----------
0            192.168.1.81      23             48000
1            10.10.1.22        23             48001
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields of the **show sessions admin**, **show sessions console**, and **show sessions telnet** displays.

### show sessions admin, show sessions console, and show sessions telnet Output

| Field | Description |
|---|---|
| Tty | The Telnet terminal number, or *console* for administrative users connected through the console port. |
| Username | Up to 30 characters of the name of an authenticated user. |
| Time (s) | Number of seconds the session has been active. |
| Type | Type of administrative session:<br>• Console<br>• SSH<br>• Telnet |

### show sessions telnet client Output

| Field | Description |
|---|---|
| Session | Session number assigned by MSS when the client session is established. |
| Server Address | IP address of the remote device. |
| Server Port | TCP port number of the remote device's TCP server. |
| Client Port | TCP port number MSS is using for the client side of the session. |

**See Also:**
• clear sessions

## show sessions network

Displays summary or verbose information about all network sessions, or network sessions for a specified username or set of usernames, MAC address or set of MAC addresses, VLAN or set of VLANs, or session ID.

**Syntax: Syntax show sessions network [user** *user-glob* **| mac-addr** *mac-addr-glob* **| ssid** *ssid-name* **| vlan** *vlan-glob* **| session-id** *session-id* **| wired] [verbose]**

**user** *user-glob* — Displays all network sessions for a single user or set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see "User Globs" on page 6.)

**mac-addr** *mac-addr-glob* — Displays all network sessions for a MAC address. Specify a MAC address in hexadecimal numbers separated by colons (:). Or use the wildcard character (*) to specify a set of MAC addresses. (For details, see "MAC Address Globs" on page 7.)


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| **ssid** *ssid-name* | Displays all network sessions for an SSID. |
| **vlan** *vlan-glob* | Displays all network sessions on a single VLAN or a set of VLANs. Specify a VLAN name, use the double-asterisk wildcard character (**) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an at sign (@) or a period (.). (For details, see “VLAN Globs” on page 6.) |
| **session-id** *local-session-id* | Displays the specified network session. To find local session IDs, use the **show sessions** command. The **verbose** option is not available with this form of the **show sessions network** command. |
| **wired** | Displays all network sessions on wired authentication ports. |
| **verbose** | Provides detailed output for all network sessions or ones displayed by username, MAC address, or VLAN name. |

**Defaults:** None.

**Access:** All.

**Usage:** MSS displays information about network sessions in three types of displays. See the following tables for field descriptions.

Summary display

Verbose display

**show sessions network session-id** display

Authorization attribute values can be changed during authorization. If the values are changed, **show sessions** output shows the values that are actually in effect following any changes.

**Examples:** To display summary information for all network sessions, type **show sessions network**. For example:

```
DWS-1008# show sessions network
User                         Sess  IP or MAC          VLAN          Port/
Name                         ID    Address            Name          Radio
---------------------------  ----  -----------------  ------------  -----
EXAMPLE\Natasha              4*    10.10.40.17        vlan-eng      3/1
host/laptop11.exmpl.com      6*    10.10.40.16        vlan-eng      3/2
nin@exmpl.com                539*  10.10.40.17        vlan-eng      1/1
EXAMPLE\hosni                302*  10.10.40.10        vlan-eng      3/1
                             563   00:0b:be:15:46:56  (none)        1/2
jose@exmpl.com               380*  10.30.40.8         vlan-eng      1/1
00:30:65:16:8d:69            443*  10.10.40.19        vlan-wep      3/1
EXAMPLE\Geetha               459*  10.10.40.18        vlan-eng      3/2

8 sessions total
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The following command displays summary information about the sessions for MAC address 00:05:5d:7e:98:1a:

```
DWS-1008# show sessions network mac-addr 00:05:5d:7e:98:1a
User                          Sess  IP or MAC        VLAN           Port/
Name                          ID    Address          Name           Radio
----------------------------  ----  ---------------  -------------  -----
EXAMPLE\Havel                 13*   10.10.10.40      vlan-eng       1/2
```

The following command displays summary information about all the sessions of users whose names begin with *E*:

```
DWS-1008# show sessions network user E*
User                          Sess  IP or MAC        VLAN           Port/
Name                          ID    Address          Name           Radio
----------------------------  ----  ---------------  -------------  -----
EXAMPLE\Singh                 12*   10.10.10.30      vlan-eng       3/2
EXAMPLE\Havel                 13*   10.10.10.40      vlan-eng       1/2
2 sessions match criteria (of 3 total)
```

The following command displays verbose output about the sessions of all current network users:

```
DWS-1008# show sessions network verbose
User                          Sess  IP or MAC        VLAN           Port/
Name                          ID    Address          Name           Radio
----------------------------  ----  ---------------  -------------  -----
SHUTTLE2\exmpl                3*    10.8.255.8       default        7/1
Client MAC: 00:0b:7d:26:b1:fb GID: SESS-3-00040c-287058-657673d4
State: ACTIVE              (prev AUTHORIZED)
now on:      172.16.0.1, port 10, AP/radio 0422900147/1, as of 00:00:22 ago
from:        172.16.0.1, port 6, AP/radio 0342900121/1, as of 00:01:07 ago
from:        172.16.0.1, port 2, AP/radio 0412900109/1, as of 00:01:53 ago

Host name: shuttle2_laptop
Vlan-Name=default (service-profile)
Service-Type=2 (service-profile)
End-Date=52/06/07-08:57 (AAA)
Start-Date=05/04/11-10:00 (AAA)

1 sessions total
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The following command displays information about network session 88:

```
DWS-1008# show sessions network session-id 88
Local Id:       88
Global Id:      SESS-88-00040f-876766-623fd6
State:          ACTIVE
SSID:           Rack-39-PM
Port/Radio:     10/1
MAC Address:        00:0f:66:f4:71:6d
User Name:      last-resort-Rack-39-PM
IP Address:     10.2.39.217
Vlan Name:      default
Tag:    1
Session Start:          Wed Apr 12 21:19:27 2006 GMT
Last Auth Time:         Wed Apr 12 21:19:26 2006 GMT
Last Activity:          Wed Apr 12 21:19:49 2006 GMT  ( <15s ago)
Session Timeout:        0
Idle Time-To-Live:      175
Login Type:             LAST-RESORT
EAP Method:             NONE, using server 172.16.0.1

Session statistics as updated from AP:
Unicast packets in: 31
Unicast bytes in: 3418
Unicast packets out: 18
Unicast bytes out: 2627
Multicast packets in: 0
Multicast bytes in: 0
Number of packets with encryption errors: 0
Number of bytes with encryption errors: 0
Last packet data rate: 48
Last packet signal strength: -60 dBm
Last packet data S/N ratio: 35
Protocol: 802.11
Session CAC: disabled
```

| Field | Description |
|---|---|
| User Name | Up to 30 characters of the name of the authenticated user of this session.<br>**Note:** For a MAC-authenticated session, this value is the client device's MAC address. |
| Sess ID | Locally unique number that identifies this session. An asterisk (*) next to a session ID indicates that the session is fully active. |
| IP or MAC Address | IP address of the session user, or the user's MAC address if the user has not yet received an IP address. |
| VLAN Name | Name of the VLAN associated with the session. |
| Port/Radio | Number of the port and radio through which the user is accessing this session. |


Download from Www.Somanuals.com. All Manuals Search And Download.

## Additional show sessions network verbose Output

| Field | Description |
|---|---|
| Client MAC | MAC address of the session user. |
| GID | Global session ID, a unique session number. |
| State | Status of the session:<br>• AUTH, ASSOC REQ—Client is being associated by the 802.1X protocol.<br>• AUTH AND ASSOC—Client is being associated by the 802.1X protocol, and the user is being authenticated.<br>• AUTHORIZING—User has been authenticated (for example, by the 802.1X protocol and an AAA method), and is entering AAA authorization.<br>• AUTHORIZED—User has been authorized by an AAA method.<br>• ACTIVE—User's AAA attributes have been applied, and the user is active on the network.<br>• DEASSOCIATED—One of the following:<br>• Wireless client has sent the switch a disassociate message.<br>• User associated with one of the current switch's access points has appeared at another switch in the Mobility Domain.<br>• ROAMING AWAY—The switch has been sent a request to transfer the user, who is roaming, to another switch.<br>• STATUS UPDATED— switch is receiving a final update from an access point about the user, who has roamed away.<br>• WEB_AUTHING—User is being authenticated by WebAAA.<br>• WIRED AUTH'ING—User is being authenticated by the 802.1X protocol on a wired authentication port.<br>• KILLING—User's session is being cleared, because of 802.1X authentication failure, entry of a **clear** command, or some other event. |
| now on | Shows the following information about the AP and radio the session is currently on:<br>• IP address and port number of the switch managing the AP<br>• Serial number and radio number of the AP<br>• Amount of time the session has been on this AP |
| from | Shows information about the APs from which the session has roamed. (See the descriptions above for the *now on* field.) |
| Host name | Host name of the user's networking device. |
| Vlan-Name (and other attributes if set) | Authorization attributes for the user and how they were assigned (the sources of the attribute values). For Vlan-Name, the source of the attribute value can be one of the following:<br>• AAA—VLAN is from RADIUS or the local database.<br>• initial-assignment—For a client that has roamed from one switch to another, VLAN is the one assigned to the user on the switch where the user first accessed the network. (This is the switch where the client's global session started.)This authorization source (initial-assignment) is displayed only if the following conditions are true:<br>• The client roamed from another switch.<br>• The service profile for the SSID the user is on is configured to keep the client's initial VLAN assignment. (This means the keep-initial-vlan option is enabled on the service profile.)<br>• The VLAN is not configured for the user on the roamed-to switch by the local database.<br>• A Location Policy on the roamed-to switch does not set the VLAN.<br>• location policy—Attribute value was assigned by a Location Policy.<br>• service-profile—Attribute value is configured on the SSID, and was not overridden by other attribute sources (such as AAA or location policy).<br>• Web Portal—Session is for a Web Portal client. |


Download from Www.Somanuals.com. All Manuals Search And Download.

## show sessions network session-id Output

| Field | Description |
|---|---|
| Local Id | Identifier for the session on this particular switch. (This is the session ID you specify when entering the **show sessions network session-id** command.) |
| Global Id | Unique session identifier within the network. |
| State | Status of the session:<br>• AUTH, ASSOC REQ—Client is being associated by the 802.1X protocol.<br>• AUTH AND ASSOC—Client is being associated by the 802.1X protocol, and the user is being authenticated.<br>• AUTHORIZING—User has been authenticated (for example, by the 802.1X protocol and an AAA method), and is entering AAA authorization.<br>• AUTHORIZED—User has been authorized by an AAA method.<br>• ACTIVE—User's AAA attributes have been applied, and the user is active on the network.<br>• DEASSOCIATED—One of the following:<br>  • Wireless client has sent the switch a disassociate message.<br>  • User associated with one of the current switch's access points has appeared at another switch in the network.<br>• STATUS UPDATED—switch is receiving a final update from an access point about the user, who has roamed away.<br>• WEB_AUTHING—User is being authenticated by WebAAA.<br>• WIRED AUTH'ING—User is being authenticated by the 802.1X protocol on a wired authentication port.<br>• KILLING—User's session is being cleared, because of 802.1X authentication failure, entry of a clear command, or some other event. |
| SSID | Name of the SSID the user is on. |
| Port/Radio | Number of the port and radio through which the user is accessing this session. |
| MAC address | MAC address of the session user. |
| User Name | Name of the authenticated user of this session |
| IP Address | IP address of the session user. |
| Vlan Name | Name of the VLAN associated with the session. |
| Tag | System-wide supported VLAN tag type. |
| Session Start | Indicates when the session started. |
| Last Auth Time | Indicates when the most recent authentication of the session occurred. |
| Last Activity | Indicates when the last activity (transmission) occurred on the session. |
| Session Timeout | Assigned session timeout in seconds. |
| Idle Time-To-Live | Number of seconds the session can remain idle before MSS changes the session state to Disassociated. |
| Login Type | Authentication type used to log onto the network:<br>• DOT1X<br>• MAC<br>• LAST-RESORT<br>• WEB-PORTA |
| EAP Method | Extensible Authentication Protocol (EAP) type used to authenticate the session user, and the IP address of the authentication server. |
| Session statistics as updated from AP | Time the session statistics were last updated from the access point, in seconds since a fixed standard date and time. |
| Unicast packets in | Total number of unicast packets received from the user by the switch (64-bit counter). |
| Unicast bytes in | Total number of unicast bytes received from the user by the switch (64-bit counter). |
| Unicast packets out | Total number of unicast packets sent by the switch to the user (64-bit counter). |


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| Unicast bytes out | Total number of unicast bytes sent by the switch to the user (64-bit counter). |
| Multicast packets in | Total number of multicast packets received from the user by the switch (64-bit counter). |
| Multicast bytes in | Total number of multicast bytes received from the user by the switch (64-bit counter). |
| Number of packets with encryption errors | Total number of decryption failures. |
| Number of bytes with encryption errors | Total number of bytes with decryption errors. |
| Last packet data rate | Data transmit rate, in megabits per second (Mbps), of the last packet received by the access point. |
| Last packet signal strength | Signal strength, in decibels referred to 1milliwatt (dBm), of the last packet received by the access point. |
| Last packet data S/N ratio | Signal-to-noise ratio of the last packet received by the access point. |
| Protocol | Wireless protocol used. |
| Session CAC | State of session-based Call Admission Control (CAC) on the SSID's service profile. |


Download from Www.Somanuals.com. All Manuals Search And Download.

# RF Detection Commands

MSS automatically performs RF detection scans on enabled and disabled radios to detect rogue access points. A rogue access point is a BSSID (MAC address associated with an SSID) that does not belong to a D-Link device and is not a member of the ignore list configured on the seed switch.

MSS can issue countermeasures against rogue devices to prevent clients from being able to use them.

You can configure RF detection parameters on individual switches.

This chapter presents RF detection commands alphabetically. Use the following table to locate the commands in this chapter based on their use.


| | |
|---|---|
| **Rogue Information** | show rfdetect clients on page 275<br>show rfdetect data on page 280<br>show rfdetect visible on page 283<br>show rfdetect counters on page 278 |
| **Countermeasures** | show rfdetect countermeasures on page 277 |
| **Permitted Vendor List** | set rfdetect vendor-list on page 274<br>show rfdetect vendor-list on page 282<br>clear rfdetect vendor-list on page 269 |
| **Permitted SSID List** | set rfdetect ssid-list on page 273<br>show rfdetect ssid-list on page 282<br>clear rfdetect ssid-list on page 269 |
| **Client Black List** | set rfdetect black-list on page 270<br>show rfdetect black-list on page 285 |
| **Attack List** | set rfdetect attack-list on page 270<br>show rfdetect attack-list on page 274<br>clear rfdetect attack-list on page 268 |
| **Ignore List** | set rfdetect ignore on page 271<br>show rfdetect ignore on page 281<br>clear rfdetect ignore on page 268 |
| **AP Signatures** | set rfdetect signature on page 272 |
| **Log Messages** | set rfdetect log on page 272 |
| **DWS-to-Client RF Link** | test rflink on page 284 |




Download from Www.Somanuals.com. All Manuals Search And Download.

# clear rfdetect attack-list

Removes a MAC address from the attack list.

**Syntax: clear rfdetect attack-list** *mac-addr*

*mac-addr* MAC address you want to remove from the attack list.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command clears MAC address 11:22:33:44:55:66 from the attack list:

```
DWS-1008# clear rfdetect attack-list 11:22:33:44:55:66
success: 11:22:33:44:55:66 is no longer in attacklist.
```

**See Also:**
- set rfdetect attack-list
- show rfdetect attack-list

# clear rfdetect ignore

Removes a device from the ignore list for RF scans. MSS does not generate log messages or traps for the devices in the ignore list.

**Syntax: clear rfdetect ignore** *mac-addr*

*mac-addr* Basic service set identifier (BSSID), which is a MAC address, of the device to remove from the ignore list.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes BSSID aa:bb:cc:11:22:33 from the ignore list for RF scans:

```
DWS-1008# clear rfdetect ignore aa:bb:cc:11:22:33
success: aa:bb:cc:11:22:33 is no longer ignored.
```

**See Also:**
- set rfdetect ignore
- show rfdetect ignore


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear rfdetect ssid-list

Removes an SSID from the permitted SSID list.

**Syntax: clear rfdetect ssid-list** *ssid-name*

*ssid-name* SSID name you want to remove from the permitted SSID list.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command clears SSID mycorp from the permitted SSID list:

```
DWS-1008# clear rfdetect ssid-list mycorp
success: mycorp is no longer in ssid-list.
```

**See Also:**
- set rfdetect ssid-list
- show rfdetect ssid-list

# clear rfdetect vendor-list

Removes an entry from the permitted vendor list.

**Syntax: clear rfdetect vendor-list {client | ap | all }** *mac-addr* **| all-macs**

**client | ap | all** Specifies whether the entry is for an AP brand or a client brand, or both types.

*mac-addr* **| all-macs** Organizationally Unique Identifier (OUI) to remove, or all of them.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes client OUI aa:bb:cc:00:00:00 from the permitted vendor list:

```
DWS-1008# clear rfdetect vendor-list client aa:bb:cc:00:00:00
success: aa:bb:cc:00:00:00 is no longer in client vendor-list.
```

**See Also:**
- set rfdetect vendor-list
- show rfdetect vendor-list


Download from Www.Somanuals.com. All Manuals Search And Download.

# set rfdetect attack-list

Adds an entry to the attack list. The attack list specifies the MAC addresses of devices that MSS should issue countermeasures against whenever the devices are detected on the network. The attack list can contain the MAC addresses of APs and clients.

**Syntax: set rfdetect attack-list** *mac-addr*

| | |
|---|---|
| *mac-addr* | MAC address you want to attack. |

**Defaults:** The attack list is empty by default.

**Access:** Enabled.

**Usage:** The attack list applies only to the switch on which the list is configured. Switches do not share attack lists.

When on-demand countermeasures are enabled (with the **set radio-profile countermeasures configured** command) only those devices configured in the attack list are subject to countermeasures. In this case, devices found to be rogues by other means, such as policy violations or by determining that the device is providing connectivity to the wired network, are not attacked.

**Examples:** The following command adds MAC address aa:bb:cc:44:55:66 to the attack list:

```
DWS-1008# set rfdetect attack-list 11:22:33:44:55:66
success:  MAC 11:22:33:44:55:66 is now in attacklist.
```

**See Also:**
- clear rfdetect attack-list
- show rfdetect attack-list
- set radio-profile countermeasures

# set rfdetect black-list

Adds an entry to the client black list. The client black list specifies clients that are not allowed on the network. MSS drops all packets from the clients on the black list.

**Syntax: set rfdetect black-list** *mac-addr*

| | |
|---|---|
| *mac-addr* | MAC address you want to place on the black list. |

**Defaults:** The client black list is empty by default.

**Access:** Enabled.

**Usage:** In addition to manually configured entries, the list can contain entries added by MSS.


Download from Www.Somanuals.com. All Manuals Search And Download.

MSS can place a client in the black list due to an association, reassociation or disassociation flood from the client.

The client black list applies only to the switch on which the list is configured. Switches do not share client black lists.

**Examples:** The following command adds client MAC address 11:22:33:44:55:66 to the black list:

```
DWS-1008# set rfdetect black-list 11:22:33:44:55:66
success:  MAC 11:22:33:44:55:66 is now blacklisted.
```

**See Also:**
- set rfdetect black-list
- show rfdetect black-list

# set rfdetect ignore

Configures a list of known devices to ignore during an RF scan. MSS does not generate log messages or traps for the devices in the ignore list.

**Syntax: set rfdetect ignore** *mac-addr*

| | |
|---|---|
| *mac-addr* | BSSID (MAC address) of the device to ignore. |

**Defaults:** MSS reports all non-D-Link BSSIDs detected during an RF scan.

**Access:** Enabled.

**Usage:** Use this command to identify third-party APs and other devices you are already aware of and do not want MSS to report following RF scans.

If you try to initiate countermeasures against a device on the ignore list, the ignore list takes precedence and MSS does not issue the countermeasures. Countermeasures apply only to rogue devices.

If you add a device that MSS has classified as a rogue to the permitted vendor list or permitted SSID list, but not to the ignore list, MSS can still classify the device as a rogue. Adding an entry to the permitted vendor list or permitted SSID list merely indicates that the device is from an allowed manufacturer or is using an allowed SSID. However, to cause MSS to stop classifying the device as a rogue, you must add the device's MAC address to the ignore list.

**Examples:** The following command configures MSS to ignore BSSID aa:bb:cc:11:22:33 during RF scans:

```
DWS-1008# set rfdetect ignore aa:bb:cc:11:22:33
success:  MAC aa:bb:cc:11:22:33 is now ignored.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

**See Also:**
• clear rfdetect ignore
• show rfdetect ignore

# set rfdetect log

Disables or reenables generation of log messages when rogues are detected or when they disappear.

**Syntax: set rfdetect log {enable | disable}**

**enable** Enables logging of rogues.

**disable** Disables logging of rogues.

**Defaults:** RF detection logging is enabled by default.

**Access:** Enabled.

**Usage:** The log messages for rogues are generated only on the seed and appear only in the seed's log message buffer. Use the **show log buffer** command to display the messages in the seed switch's log message buffer.

**Examples:** The following command enables RF detection logging for the Mobility Domain managed by this seed switch:

```
DWS-1008# set rfdetect log enable
success:  rfdetect logging is enabled.
```

**See Also:**
• show log buffer

# set rfdetect signature

Enables AP signatures. An AP signature is a set of bits in a management frame sent by an AP that identifies that AP to MSS. If someone attempts to spoof management packets from a D-Link AP, MSS can detect the spoof attempt.

**Syntax: set rfdetect signature {enable | disable}**

**enable** Enables AP signatures.

**disable** Disables AP signatures.

**Defaults:** AP signatures are disabled by default.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** The command applies only to APs managed by the switch on which you enter the command. To enable signatures on all APs, enter the command on each switch.

**Note:** You must use the same AP signature setting (enabled or disabled) on all switches.

**Examples:** The following command enables AP signatures on an switch:

```
DWS-1008# set rfdetect signature enable
success:  signature is now enabled.
```

## set rfdetect ssid-list

Adds an SSID to the permitted SSID list. The permitted SSID list specifies the SSIDs that are allowed on the network. If MSS detects packets for an SSID that is not on the list, the AP that sent the packets is classified as a rogue. MSS issues countermeasures against the rogue if they are enabled.

**Syntax: set rfdetect ssid-list** *ssid-name*

| | |
|---|---|
| *ssid-name* | SSID name you want to add to the permitted SSID list. |

**Defaults:** The permitted SSID list is empty by default and all SSIDs are allowed. However, after you add an entry to the list, MSS allows traffic only for the SSIDs that are on the list.

**Access:** Enabled.

**Usage:** The permitted SSID list applies only to the switch on which the list is configured. Switches do not share permitted SSID lists.

If you add a device that MSS has classified as a rogue to the permitted SSID list, but not to the ignore list, MSS can still classify the device as a rogue. Adding an entry to the permitted SSID list merely indicates that the device is using an allowed SSID. However, to cause MSS to stop classifying the device as a rogue, you must add the device's MAC address to the ignore list.

**Examples:** The following command adds SSID *mycorp* to the list of permitted SSIDs:

```
DWS-1008# set rfdetect ssid-list mycorp
success:  ssid mycorp is now in ssid-list.
```

**See Also:**
- clear rfdetect ssid-list
- show rfdetect ssid-list


Download from Www.Somanuals.com. All Manuals Search And Download.

# set rfdetect vendor-list

Adds an entry to the permitted vendor list. The permitted vendor list specifies the third-party AP or client vendors that are allowed on the network. MSS does not list a device as a rogue or interfering device if the device's OUI is in the permitted vendor list.

**Syntax: set rfdetect vendor-list {client | ap}** *mac-addr*

**client | ap** Specifies whether the entry is for an AP brand or a client brand.

*mac-addr* **| all** Organizationally Unique Identifier (OUI) to remove.

**Defaults:** The permitted vendor list is empty by default and all vendors are allowed. However, after you add an entry to the list, MSS allows only the devices whose OUIs are on the list.

**Access:** Enabled.

**Usage:** The permitted vendor list applies only to the switch on which the list is configured. Switches do not share permitted vendor lists.

If you add a device that MSS has classified as a rogue to the permitted vendor list, but not to the ignore list, MSS can still classify the device as a rogue. Adding an entry to the permitted vendor list merely indicates that the device is from an allowed vendor. However, to cause MSS to stop classifying the device as a rogue, you must add the device's MAC address to the ignore list.

**Examples:** The following command adds an entry for clients whose MAC addresses start with aa:bb:cc:

```
DWS-1008# set rfdetect vendor-list client aa:bb:cc:00:00:00
success:  MAC aa:bb:cc:00:00:00 is now in client vendor-list.
```

The trailing 00:00:00 value is required.

# show rfdetect attack-list

Displays information about the MAC addresses in the attack list.

**Syntax: show rfdetect attack-list**

**Defaults:** None.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following example shows the attack list on switch:

```
DWS-1008# show rfdetect attack-list
Total number of entries: 1
Attacklist MAC      Port/Radio/Chan     RSSI    SSID
------------------  ------------------  ------  ------------
11:22:33:44:55:66   dap 2/1/11          -53     rogue-ssid
```

**See Also:**
- clear rfdetect attack-list
- set rfdetect attack-list

# show rfdetect black-list

Displays information abut the clients in the client black list.

**Syntax: show rfdetect black-list**

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following example shows the client black list on switch:

```
DWS-1008# show rfdetect black-list
Total number of entries: 1
Blacklist MAC       Type                Port    TTL
------------------  ------------------  ------  ------------
11:22:33:44:55:66   configured          -       -
11:23:34:45:56:67   assoc req flood     3       25
```

**See Also:**
- clear rfdetect black-list
- set rfdetect black-list

# show rfdetect clients

Displays the wireless clients detected by a switch.

**Syntax: show rfdetect clients [mac** *mac-addr***]**

**mac** *mac-addr* Displays detailed information for a specific client.

**Defaults:** None.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command shows information about all wireless clients detected by a switch's APs:

```
DWS-1008# show rfdetect clients
Total number of entries: 30
Client MAC         Client Vendor  AP MAC            AP Vendor  Port/Radio /Channel  NoL  Type   Last seen
-----------------  -------        ----------------- -------    -------------        ---  -----  ----
00:03:7f:bf:16:70  Unknown        Unknown                      dap 1/1/6            1    intfr  207
00:04:23:77:e6:e5  Intel          Unknown                      dap 1/1/2            1    intfr  155
00:05:5d:79:ce:0f  D-Link         Unknown                      dap1/1/149           1    intfr  87
00:05:5d:7e:96:a7  D-Link         Unknown                      dap1/1/149           1    intfr  117
00:05:5d:7e:96:ce  D-Link         Unknown                      dap1/1/157           1    intfr  162
00:05:5d:84:d1:c5  D-Link         Unknown                      dap 1/1/1            1    intfr  52
```

The following command displays more details about a specific client:

```
DWS-1008# show rfdetect clients mac 00:0c:41:63:fd:6d
Client Mac Address: 00:0c:41:63:fd:6d, Vendor: Linksys  Port: dap 1, Radio: 1, Channel:
11, RSSI: -82, Rate: 2, Last Seen (secs ago): 84
Bssid: 00:0b:0e:01:02:00, Vendor: D-Link, Type: intfr, Dst: ff:ff:ff:ff:ff:ff
Last Rogue Status Check (secs ago): 3
```

The first line lists information for the client. The other lines list information about the most recent 802.11 packet detected from the client.

## show rfdetect clients Output

| Field | Description |
|---|---|
| Client MAC | MAC address of the client. |
| Client Vendor | Company that manufactures or sells the client. |
| AP MAC | MAC address of the radio with which the rogue client is associated. |
| AP Vendor | Company that manufactures or sells the AP with which the rogue client is associated. |
| Port/Radio/Channel | Port number, radio number, and channel number of the radio that detected the rogue. For a Distributed AP, the connection number is labeled dap. (This stands for *distributed ap*.) |
| NoL | Number of listeners. This is the number of AP radios that detected the rogue client. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| Type | Classification of the rogue device:<br>• rogue—Wireless device that is on the network but is not supposed to be on the network.<br>• intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with AP radios.<br>• known—Device that is a legitimate member of the network. |
| Last seen | Number of seconds since an AP radio last detected 802.11 packets from the device. |

### show rfdetect clients mac Output

| Field | Description |
|---|---|
| RSSI | Received signal strength indication (RSSI)—the strength of the RF signal detected by the AP radio, in decibels referred to 1 milliwatt (dBm). |
| Rate | The data rate of the client. |
| Last Seen | Number of seconds since an AP radio last detected 802.11 packets from the device. |
| BSSID | MAC address of the SSID with which the rogue client is associated. |
| Vendor | Company that manufactures or sells the AP with which the rogue client is associated. |
| Typ | Classification of the rogue device:<br>• rogue—Wireless device that is on the network but is not supposed to be on the network.<br>• intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with AP radios.<br>• known—Device that is a legitimate member of the network. |
| Dst | MAC addressed to which the last 802.11 packet detected from the client was addressed. |
| Last Rogue Status Check | Number of seconds since the switch looked on the air for the AP with which the rogue client is associated. The switch looks for the client's AP by sending a packet from the wired side of the network addressed to the client, and watching the air for a wireless packet containing the client's MAC address. |

## show rfdetect countermeasures

Displays the current status of countermeasures against rogues.

**Syntax: show rfdetect countermeasures**

**Defaults:** None.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** This command is valid only on the seed switch

**Examples:** The following example displays countermeasures status:

```
DWS-1008# show rfdetect countermeasures
Total number of entries: 190
Rogue MAC         Type   Countermeasures    IPaddr          Port/Radio
                         Radio Mac                          /Channel
----------------  -----  -----------------  --------------  -------------
00:0b:0e:00:71:c0 intfr  00:0b:0e:44:55:66   10.1.1.23       dap 4/1/6
00:0b:0e:03:00:80 rogue  00:0b:0e:11:22:33   10.1.1.23       dap 2/1/11
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Rogue MAC | BSSID of the rogue. |
| Type | Classification of the rogue device:<br>• rogue—Wireless device that is on the network but is not supposed to be on the network.<br>• intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with AP radios.<br>• known—Device that is a legitimate member of the network. |
| Countermeasures Radio MAC | MAC address of the D-Link radio sending countermeasures against the rogue. |
| IPaddr | System IP address of the switch that is managing the AP that is sending or will send countermeasures. |
| Port/Radio/Channel | Port number, radio number, and channel number of the countermeasures radio. For a Distributed AP, the connection number is labeled *dap*. (This stands for *distributed ap*.) |

**See Also:**
• set radio-profile countermeasures

# show rfdetect counters

Displays statistics for rogue and Intrusion Detection System (IDS) activity detected by the APs managed by a switch.

**Syntax: show rfdetect counters**

**Defaults:** None.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command shows counters for rogue activity detected by a switch:

DWS-1008# **show rfdetect countermeasures**

| Type | Current | Total |
|---|---|---|
| Rogue access points | 0 | 0 |
| Interfering access points | 139 | 1116 |
| Rogue 802.11 clients | 0 | 0 |
| Interfering 802.11 clients | 4 | 347 |
| 802.11 adhoc clients | 0 | 1 |
| Unknown 802.11 clients | 20 | 965 |
| Interfering 802.11 clients seen on wired network | 0 | 0 |
| 802.11 probe request flood | 0 | 0 |
| 802.11 authentication flood | 0 | 0 |
| 802.11 null data flood | 0 | 0 |
| 802.11 mgmt type 6 flood | 0 | 0 |
| 802.11 mgmt type 7 flood | 0 | 0 |
| 802.11 mgmt type d flood | 0 | 0 |
| 802.11 mgmt type e flood | 0 | 0 |
| 802.11 mgmt type f flood | 0 | 0 |
| 802.11 association flood | 0 | 0 |
| 802.11 reassociation flood | 0 | 0 |
| 802.11 disassociation flood | 0 | 0 |
| Weak wep initialization vectors | 0 | 0 |
| Spoofed access point mac-address attacks | 0 | 0 |
| Spoofed client mac-address attacks | 0 | 0 |
| Ssid masquerade attacks | 1 | 12 |
| Spoofed deauthentication attacks | 0 | 0 |
| Spoofed disassociation attacks | 0 | 0 |
| Null probe responses | 626 | 11380 |
| Broadcast deauthentications | 0 | 0 |
| FakeAP ssid attacks | 0 | 0 |
| FakeAP bssid attacks | 0 | 0 |
| Netstumbler clients | 0 | 0 |
| Wellenreiter clients | 0 | 0 |
| Active scans | 1796 | 4383 |
| Wireless bridge frames | 196 | 196 |
| Adhoc client frames | 8 | 0 |
| Access points present in attack-list | 0 | 0 |
| Access points not present in ssid-list | 0 | 0 |
| Access points not present in vendor-list | 0 | 0 |
| Clients not present in vendor-list | 0 | 0 |
| Clients added to automatic black-list | 0 | 0 |


Download from Www.Somanuals.com. All Manuals Search And Download.

# show rfdetect data

Displays information about the APs detected by a switch.

**Syntax: show rfdetect data**

**Defaults:** None.

**Access:** Enabled.

**Usage:** You can enter this command on any switch. The output applies only to the switch on which you enter the command. To display all devices that a specific D-Link radio has detected, even if the radio is managed by another switch, use the **show rfdetect visible** command.

Only one MAC address is listed for each D-Link radio, even if the radio is beaconing multiple SSIDs.

**Examples:** The following command shows the devices detected by this switch during the most recent RF detection scan:

```
DWS-1008# show rfdetect data
Total number of entries: 197
Flags: i = infrastructure, a = ad-hoc
c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
BSSID              Vendor  Type  Port/Radio  Flags  RSSI  Age  SSID
                                 /Ch
-----------------  -------  ----  ----------  ------  ----  ---  -----------------
00:07:50:d5:cc:91  Cisco    intfr  3/1/6      i----w  -61   6    r27-cisco1200-2
00:07:50:d5:dc:78  Cisco    intfr  3/1/6      i----w  -82   6    r116-cisco1200-2
00:09:b7:7b:8a:54  Cisco    intfr  3/1/2      i-----  -57   6
00:0a:5e:4b:4a:c0  3Com     intfr  3/1/11     i-----  -57   6    public
00:0a:5e:4b:4a:c2  3Com     intfr  3/1/11     i-t1--  -86   6    trapezewlan
00:0a:5e:4b:4a:c4  3Com     intfr  3/1/11     ic----  -85   6    trpz-ccmp
00:0a:5e:4b:4a:c6  3Com     intfr  3/1/11     i-t---  -85   6    trpz-tkip
00:0a:5e:4b:4a:c8  3Com     intfr  3/1/11     i----w  -83   6    trpz-voip
00:0a:5e:4b:4a:ca  3Com     intfr  3/1/11     i-----  -85   6    trpz-webaaa
...
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields in this display.

| Field | Description |
|---|---|
| BSSID | MAC address of the SSID used by the detected device. |
| Vendor | Company that manufactures or sells the rogue device. |
| Type | Classification of the rogue device:<br>• rogue—Wireless device that is not supposed to be on the network. The device has an entry in a switch's FDB and is therefore on the network.<br>• intfr—Wireless device that is not part of your network but is not a rogue. The device does not have an entry in a switch's FDB and is not actually on the network, but might be causing RF interference with AP radios.<br>• known—Device that is a legitimate member of the network. |
| Port/Radio/Channel | Port number, radio number, and channel number of the radio that detected the rogue. For a Distributed AP, the connection number is labeled *dap*. (This stands for *distributed ap*.) |
| Flags | Classification and encryption information for the rogue:<br>• The i, a, or u flag indicates the classification.<br>• The other flags indicate the encryption used by the rogue.<br>For flag definitions, see the key in the command output. |
| RSSI | Received signal strength indication (RSSI)—the strength of the RF signal detected by the AP radio, in decibels referred to 1 milliwatt (dBm). |
| Age | Number of seconds since an AP radio last detected 802.11 packets from the device. |

**See Also:**
• show rfdetect visible

# show rfdetect ignore

Displays the BSSIDs of third-party devices that MSS ignores during RF scans. MSS does not generate log messages or traps for the devices in the ignore list.

**Syntax: show rfdetect ignore**

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following example displays the list of ignored devices:

```
DWS-1008# show rfdetect ignore
Total number of entries: 2
Ignore MAC
-----------------
aa:bb:cc:11:22:33
aa:bb:cc:44:55:66
```

**See Also:**
• clear rfdetect ignore
• set rfdetect ignore


Download from Www.Somanuals.com. All Manuals Search And Download.

# show rfdetect ssid-list

Displays the entries in the permitted SSID list.

**Syntax: show rfdetect ssid-list**

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following example shows the permitted SSID list on switch:

```
DWS-1008# show rfdetect ssid-list
Total number of entries: 3
SSID
-----------------
mycorp
corporate
guest
```

**See Also:**
- clear rfdetect ssid-list
- set rfdetect ssid-list

# show rfdetect vendor-list

Displays the entries in the permitted vendor list.

**Syntax: show rfdetect vendor-list**

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following example shows the permitted vendor list on switch:

```
DWS-1008# show rfdetect vendor-list
Total number of entries: 1
      OUI               Type
-----------------       ------
aa:bb:cc:00:00:00   client
11:22:33:00:00:00   ap
```

**See Also:**
- clear rfdetect vendor-list
- set rfdetect vendor-list


Download from Www.Somanuals.com. All Manuals Search And Download.

# show rfdetect visible

Displays the BSSIDs discovered by a specific D-Link radio. The data includes BSSIDs transmitted by other D-Link radios as well as by third-party access points.

**Syntax: show rfdetect visible** *mac-addr*

**Syntax: show rfdetect visible ap** *mp-num* **[radio{1|2}]**

**Syntax: show rfdetect visible dap** *dap-num* **[radio{1|2}]**

| | |
|---|---|
| *mac-addr* | Base MAC address of the D-Link radio.<br>**Note:** To display the base MAC address of a D-Link radio, use the **show{ap\|dap}status** command. |
| *mp-num* | Port connected to the AP access point for which to display neighboring BSSIDs. |
| *dap-num* | Number of a Distributed AP for which to display neighboring BSSIDs. |
| **radio 1** | Shows neighbor information for radio 1. |
| **radio 2** | Shows neighbor information for radio 2. (This option does not apply to single-radio models.) |

**Defaults:** None.

**Access:** Enabled.

**Usage:** If a D-Link radio is supporting more than one SSID, each of the corresponding BSSIDs is listed separately.

**Examples:** To following command displays information about the rogues detected by radio 1 on AP port 3:

```
DWS-1008# show rfdetect visible ap 3 radio 1
Total number of entries: 104
Flags: i = infrastructure, a = ad-hoc
       c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
Transmit MAC      Vendor   Type  Ch  RSSI  Flags   SSID
----------------- -------  ----- --- ----  ------  --------------------------------
00:07:50:d5:cc:91 Cisco    intfr 6   -60   i----w  r27-cisco1200-2
00:07:50:d5:dc:78 Cisco    intfr 6   -82   i----w  r116-cisco1200-2
00:0a:5e:4b:4a:c8 3Com     intfr 11  -83   i----w trpz-voip
00:0a:5e:4b:4a:ca 3Com     intfr 11   -85  i----- trpz-webaaa
...
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Transmit MAC | MAC address the rogue device that sent the 802.11 packet detected by the AP radio |
| Vendor | Company that manufactures or sells the rogue device. |
| Type | Classification of the rogue device:<br>• rogue—Wireless device that is on the network but is not supposed to be on the network.<br>• intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with AP radios.<br>• known—Device that is a legitimate member of the network. |
| Ch | Channel number on which the radio detected the rogue. |
| RSSI | Received signal strength indication (RSSI)—the strength of the RF signal detected by the AP radio, in decibels referred to 1 milliwatt (dBm). |
| Flags | Classification and encryption information for the rogue:<br>• The i, a, or u flag indicates the classification.<br>• The other flags indicate the encryption used by the rogue.<br>For flag definitions, see the key in the command output. |
| SSID | SSID used by the detected device. |

**See Also:**
• show rfdetect data

# test rflink

Provides information about the RF link between the switch and the client based on sending test packets to the client.

**Syntax: test rflink {mac** *mac-addr* **| session-id** *session-id***}**

| | |
|---|---|
| *mac-addr* | Tests the RF link between the switch and the client with the specified MAC address. |
| *session-id* | Tests the RF link between the switch and the client with the specified local session ID. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** Use this command to send test packets to a specified client. The output of the command indicates the number of test packets received and acknowledged by the client, as well as the client's signal strength and signal-to-noise ratio.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command tests the RF link between the switch and the client with MAC address 00:0e:9b:bf:ad:13:

```
DWS-1008# test rflink mac 00:0e:9b:bf:ad:13
RF-Link Test to 00:0e:9b:bf:ad:13 :
Session-Id: 2
Packets Sent     Packets Rcvd     RSSI      SNR   RTT (micro-secs)
------------     ------------     -------   -----  ----------------
20               20               -68       26     976
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Packets Sent | The number of test packets sent from the switch to the client. |
| Packets Rcvd | The number of test packets acknowledged by the client. |
| RSSI | Received signal strength indication (RSSI)—the strength of the RF signal from the client, in decibels referred to 1 milliwatt (dBm). |
| SNR | Signal-to-noise ratio (SNR), in decibels (dB), of the data received from the client. |
| RTT (micro-secs) | The round-trip time, in microseconds, for the client response to the test packets. |

**See Also:**
- show show rfdetect data
- show rfdetect visible


Download from Www.Somanuals.com. All Manuals Search And Download.

# File Management Commands

Use file management commands to manage system files and to display software and boot information. This chapter presents file management commands alphabetically. Use the following table to locate commands in this chapter based on their use.


| | |
|---|---|
| **Software Version** | reset system on page 297<br>show version on page 304 |
| **Boot Settings** | set boot partition on page 302<br>set boot configuration-file on page 301<br>set boot backup-configuration on page 301<br>show boot on page 302<br>clear boot config on page 288<br>clear boot backup-configuration on page 288 |
| **File Management** | dir on page 292<br>copy on page 289<br>md5 on page 296<br>delete on page 291<br>mkdir on page 296<br>rmdir on page 299 |
| **Configuration File** | save config on page 300<br>load config on page 295<br>show config on page 303 |
| **System Backup and Restore** | backup on page 287<br>restore on page 298 |
| **Sygate On-Demand Agent (SODA) file installation and removal** | install soda agent on page 294<br>uninstall soda agent on page 306 |




Download from Www.Somanuals.com. All Manuals Search And Download.

# backup

Creates an archive of switch system files and optionally, user file, in Unix *tape archive* (*tar*) format.

**Syntax: backup system [tftp:/***ip-addr/***]***filename* **[all | critical]**

| | |
|---|---|
| *[***tftp:/***ip-addr/]filename* | Name of the archive file to create. You can store the file locally in the switch's nonvolatile storage or on a TFTP server. |
| **all** | Backs up system files and all the files in the user files area. The user files area contains the set of files listed in the file section of **dir** command output. |
| **critical** | Backs up system files only, including the configuration file used when booting, and certificate files. The size of an archive created by this option is generally 1MB or less. |

**Defaults:** The default is **all**.

**Access:** Enabled.

**Usage:** You can create an archive located on a TFTP server or in the switch's nonvolatile storage. If you specify a TFTP server as part of the filename, the archive is copied directly to the TFTP server and not stored locally on the switch.

Use the **critical** option if you want to back up or restore only the system-critical files required to operate and communicate with the switch. Use the **all** option if you also want to back up or restore WebAAA pages, backup configuration files, image files, and any other files stored in the user files area of nonvolatile storage.

The maximum supported file size is 32MB. If the file size of the tarball is too large, delete unnecessary files (such as unneeded copies of system image files) and try again, or use the **critical** option instead of the **all** option.

Neither option archives image files or any other files listed in the *Boot* section of **dir** command output. The **all** option archives image files only if they are present in the user files area.

Archive files created by the **all** option are larger than files created by the **critical** option. The file size depends on the files in the user area, and the file can be quite large if the user area contains image files.

The **backup** command places the boot configuration file into the archive. (The boot configuration file is the *Configured boot configuration* in the **show boot** command's output.) If the running configuration contains changes that have not been saved, these changes are not in the boot configuration file and are not archived. To make sure the archive contains the configuration that is currently running on the switch, use the **save config** command to save the running configuration to the boot configuration file, before using the **backup** command.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command creates an archive of the system-critical files and copies the archive directly to a TFTP server. The filename in this example includes a TFTP server IP address, so the archive is not stored locally on the switch.

```
DWS-1008# backup system tftp:/10.10.20.9/sysa_bak critical
success: sent 28263 bytes in 0.324 seconds [ 87231 bytes/sec]
```

**See Also:**
- dir
- restore

# clear boot backup-configuration

Clears the filename specified as the backup configuration file. In the event that MSS cannot read the configuration file at boot time, a backup configuration file is not used.

**Syntax: clear boot backup-configuration**

**Defaults:** None.

**Access:** Enabled.

**Usage:** You can create an archive located on a TFTP server or in the switch's nonvolatile storage. If you specify a TFTP server as part of the filename, the archive is copied directly to the TFTP server and not stored locally on the switch.

**Examples:** The following command clears the name specified as the backup configuration file from the configuration of the switch:

```
DWS-1008# clear boot backup-configuration
success: Backup boot config filename was cleared.
```

**See Also:**
- set boot backup-configuration
- show boot

# clear boot config

Resets to the factory default the configuration that MSS loads during a reboot.

**Syntax: clear boot config**

**Defaults:** None.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following commands back up the configuration file on a switch, reset the switch to its factory default configuration, and reboot the switch:

```
DWS-1008# copy configuration tftp://10.1.1.1/backupcfg
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]

DWS-1008# clear boot config
success: Reset boot config to factory defaults.

DWS-1008# reset system force
..... rebooting .....
```

# copy

Performs the following copy operations:

- Copies a file from a TFTP server to nonvolatile storage.
- Copies a file from nonvolatile storage or temporary storage to a TFTP server.
- Copies a file from one area in nonvolatile storage to another.
- Copies a file to a new filename in nonvolatile storage.

**Syntax: copy** *source-url destination-url*

| | |
|---|---|
| *source-url* | Name and location of the file to copy. The uniform resource locator (URL) can be one of the following:<br>• [*subdirname/*]*filename*<br>• file:[*subdirname/*]*filename*<br>• tftp://*ip-addr*/[*subdirname/*]*filename*<br>• tmp:*filename*<br><br>For the filename, specify between 1 and 128 alphanumeric characters, with no spaces. Enter the IP address in dotted decimal notation. The *subdirname/* option specifies a subdirectory. |
| *destination-url* | Name of the copy and the location where to place the copy. The URL can be one of the following:<br>• [*subdirname/*]*filename*<br>• file:[*subdirname/*]*filename*<br>• tftp://*ip-addr*/[*subdirname/*]*filename*<br>If you are copying a system image file into nonvolatile storage, the filename must include the boot partition name. You can specify one of the following:<br>• **boot0:**/filename<br>• **boot1:**/filename |

**Defaults:** None.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** The *filename* and **file:***filename* URLs are equivalent. You can use either URL to refer to a file in a switch's nonvolatile memory. The **tftp:***//ip-addr/filename* URL refers to a file on a TFTP server. If DNS is configured on the switch, you can specify a TFTP server's hostname as an alternative to specifying the IP address.

The **tmp:***filename* URL specifies a file in temporary storage. You can copy a file out of temporary storage but you cannot copy a file into temporary storage. Temporary storage is reserved for use by MSS.

If you are copying a system image file into nonvolatile storage, the filename must be preceded by the boot partition name, which can be **boot0** or **boot1**. Enter the filename as **boot0:***/filename* or **boot1:***/filename*. You must specify the boot partition that was not used to load the currently running image.

The maximum supported file size for TFTP is 32MB.
**Examples:** The following command copies a file called *floormx* from nonvolatile storage to a TFTP server:

```
DWS-1008# copy floormx tftp://10.1.1.1/floormx
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
```

The following command copies a file called *closetmx* from a TFTP server to nonvolatile storage:

```
DWS-1008# copy tftp://10.1.1.1/closetmx closetmx
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

The following command copies system image *MX020101.020* from a TFTP server to boot partition 1 in nonvolatile storage:

```
DWS-1008# copy tftp://10.1.1.107/MX020101.020 boot1:MX020101.020
.....success: received 9163214 bytes in 105.939 seconds [ 86495 bytes/sec]
```

The following commands rename *test-config* to *new-config* by copying it from one name to the other in the same location, then deleting *test-config*:

```
DWS-1008# copy test-config new-config
DWS-1008# delete test-config
success: file deleted.
```

The following command copies file *corpa-login.html* from a TFTP server into subdirectory *corpa* in a switch's nonvolatile storage:

```
DWS-1008# copy tftp://10.1.1.1/corpa-login.html corpa/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

**See Also:**
- delete
- dir


Download from Www.Somanuals.com. All Manuals Search And Download.

# delete

**Caution:** MSS does not prompt you to verify whether you want to delete a file. When you press Enter after typing a delete command, MSS immediately deletes the specified file.

**Note:** MSS does not allow you to delete the currently running software image file or the running configuration.

**Syntax: delete** *url*

| | |
|---|---|
| *url* | Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.<br><br>If the file is in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename.<br>For example: **subdir_a/file_a.** |

**Defaults:** None.

**Access:** Enabled.

**Usage:** You might want to copy the file to a TFTP server as a backup before deleting the file.

**Examples:** The following commands copy file testconfig to a TFTP server and delete the file from nonvolatile storage:

```
DWS-1008# copy testconfig tftp://10.1.1.1/testconfig
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]

DWS-1008# delete testconfig
success: file deleted.
```

**Examples:** The following command deletes file *dang_doc* from subdirectory *dang*:

```
DWS-1008# delete dang/dang_doc
success: file deleted.
```

**See Also:**
- copy
- dir


Download from Www.Somanuals.com. All Manuals Search And Download.

# dir

Displays a list of the files in nonvolatile storage and temporary files.

**Syntax: dir [*subdirname*] | [file:] | [core:] | [boot0:] | [boot1:]**

| | |
|---|---|
| *subdirname* | Subdirectory name. If you specify a subdirectory name, the command lists the files in that subdirectory. Otherwise, the command lists the files in the root directory and also lists the subdirectories. |
| **file:** | Limits **dir** output to the contents of the user files area |
| **core:** | Limits dir output to the contents of the /tmp/core subdirectory |
| **boot0:** | Limits **dir** output to the contents of the *boot0* partition |
| **boot1:** | Limits **dir** output to the contents of the *boot1* partition |

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command displays the files in the root directory:

```
DWS-1008# dir
=============================================================
file:
Filename                          Size        Created
file:configuration                48 KB       Jul 12 2005, 15:02:32
file:corp2:corp2cnfig             17 KB       Mar 14 2005, 22:20:04
corp_a/                           512 bytes   May 21 2004, 19:15:48
file:dangcfg                      14 KB       Mar 14 2005, 22:20:04
old/                              512 bytes   May 16 2004, 17:23:44
file:pubsconfig-april062005       40 KB       May 09 2005, 21:08:30
file:sysa_bak                     12 KB       Mar 15 2005, 19:18:44
file:testback                     28 KB       Apr 19 2005, 16:37:18
Total:      159 Kbytes used, 207663 Kbytes free
=============================================================
Boot:
Filename                          Size        Created
boot0:mx040100.020                9780 KB     Aug 23 2005, 15:54:08
*boot1:mx040100.020               9796 KB     Aug 28 2005, 21:09:56
Boot0: Total:     9780 Kbytes used, 2460 Kbytes free
Boot1: Total:     9796 Kbytes used, 2464 Kbytes free
=============================================================
temporary files:
Filename                          Size        Created
```


Download from Www.Somanuals.com. All Manuals Search And Download.

```
core:command_audit.cur                  37 bytes     Aug 28 2005, 21:11:41
Total:        37 bytes used, 91707 Kbytes free
```

The following command displays the files in the root directory:

```
DWS-1008# dir file:
============================================================
file:
Filename                                Size         Created
file:configuration                      48 KB        Jul 12 2005, 15:02:32
file:corp2:corp2cnfig                   17 KB        Mar 14 2005, 22:20:04
corp_a/                                 512 bytes    May 21 2004, 19:15:48
file:dangcfg                            14 KB        Mar 14 2005, 22:20:04
dangdir/                                512 bytes    May 16 2004, 17:23:44
file:pubsconfig-april062005             40 KB        May 09 2005, 21:08:30
file:sysa_bak                           12 KB        Mar 15 2005, 19:18:44
file:testback                           28 KB        Apr 19 2005, 16:37:18
Total:        159 Kbytes used, 207663 Kbytes free
```

The following command limits the output to the contents of the */tmp/core* subdirectory:

```
DWS-1008# dir core:
============================================================
file:
Filename                                Size         Created
core:command_audit.cur                   37 bytes    Aug 28 2005, 21:11:41
Total:        37 bytes used, 91707 Kbytes free
```

The following command limits the output to the contents of the *boot0* partition:

```
DWS-1008# dir boot0:
============================================================
file:
Filename                                Size         Created
boot0:mx040100.020                      9780 KB      Aug 23 2005, 15:54:08
Total:        9780 Kbytes used, 207663 Kbytes free
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields in the **dir** output.

| Field | Description |
|---|---|
| Filename | Filename or subdirectory name.<br>For files, the directory name is shown in front of the filename (for example, file: configuration). The file: directory is the root directory.<br>For subdirectories, a forward slash is shown at the end of the subdirectory name (for example, old/).<br>In the boot partitions list (Boot:), an asterisk (*) indicates the boot partition from which the currently running image was loaded and the image filename. |
| Size | Size in Kbytes or bytes. |
| Created | System time and date when the file was created or copied onto the switch. |
| Total | Number of kilobytes in use to store files and the number that are still free. |

# install soda agent

Installs Sygate On-Demand (SODA) agent files in a directory on the switch.

**Syntax: install soda agent** *agent-file* **agent-directory** *directory*

| | |
|---|---|
| *agent-file* | Name of a .zip file on the switch containing SODA agent files. |
| *directory* | Directory on the switch where SODA agent files are to be installed. The command automatically creates this directory. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** Use this command to install a .zip file containing SODA agent files into a directory on the switch. Prior to installing the SODA agent files, you must have already copied the .zip file to the switch. This command creates the specified directory, unzips the file and places the contents into the directory. If the specified directory has the same name as an SSID, then that SSID uses the SODA agent files in the directory if SODA functionality is enabled for the service profile that manages the SSID.

**Examples:** The following command installs the contents of the file *soda.ZIP* into a directory called *sp1*.

```
DWS-1008# install soda agent soda.ZIP agent-directory sp1
This command may take up to 20 seconds...
```

**See Also:**
- uninstall soda agent
- set service-profile soda mode


Download from Www.Somanuals.com. All Manuals Search And Download.

# load config

**Caution:** This command completely removes the running configuration and replaces it with the configuration contained in the file. D-Link recommends that you save a copy of the current running configuration to a backup configuration file before loading a new configuration.

Loads configuration commands from a file and replaces the switch's running configuration with the commands in the loaded file.

**Syntax: load config [*url*]**

| | |
|---|---|
| *url* | Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.<br>If the file is in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: **backup_configs/config_c.** |

**Defaults:** The default file location is nonvolatile storage.

**Note:** The current version supports loading a configuration file only from the switch's nonvolatile storage. You cannot load a configuration file directly from a TFTP server.

If you do not specify a filename, MSS uses the same configuration filename that was used for the previous configuration load. For example, if the switch used configuration for the most recent *configuration* load, MSS uses configuration again unless you specify a different filename. To display the filename of the *configuration* file MSS loaded during the last reboot, use the **show boot** command.

**Access:** Enabled.

**Usage:** This command completely replaces the running configuration with the configuration in the file.

**Examples:** The following command reloads the configuration from the most recently loaded configuration file:

```
DWS-1008# load config
Reloading configuration may result in lost of connectivity, do you wish to continue? (y/n) [n]y
success: Configuration reloaded
```

The following command loads configuration file *testconfig1*:

```
DWS-1008# load config testconfig1
Reloading configuration may result in lost of connectivity, do you wish to continue? (y/n) [n]y
success: Configuration reloaded
```

**See Also:**
- save config
- show boot
- show config


Download from Www.Somanuals.com. All Manuals Search And Download.

# md5

Calculates the MD5 checksum for a file in the switch's nonvolatile storage.

**Syntax: md5 [boot0: | boot1:]***filename*

**boot0: | boot1:** Boot partition into which you copied the file.

*filename:* Name of the file.

**Defaults:** None.

**Access:** Enabled.

**Usage:** You must include the boot partition name in front of the filename. If you specify only the filename, the CLI displays a message stating that the file does not exist.

**Examples:** The following command calculates the checksum for image file MX040003.020 in boot partition 0:

```
DWS-1008# md5 boot0:MX040003.020
MD5 (boot0:MX040003.020) = b9cf7f527f74608e50c70e8fb896392a
```

**See Also:**
- copy
- dir

# mkdir

Creates a new subdirectory in nonvolatile storage.

**Syntax: mkdir [***subdirname***]**

*subdirname:* Subdirectory name. Specify between 1 and 32 alphanumeric characters, with no spaces.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following commands create a subdirectory called *corp2* and display the root directory to verify the result:

```
DWS-1008# mkdir corp2
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

```
DWS-1008# dir
==========================================================
file:
Filename                                Size        Created
file:configuration                      17 KB       May 21 2004, 18:20:53
file:configuration.txt                  379 bytes   May 09 2004, 18:55:17
corp2/                                  512 bytes   May 21 2004, 19:22:09
corp_a/                                 512 bytes   May 21 2004, 19:15:48
file:dangcfg                            13 KB       May 16 2004, 18:30:44
dangdir/                                512 bytes   May 16 2004, 17:23:44
old/                                    512 bytes   Sep 23 2003, 21:58:48
Total:      33 Kbytes used, 207822 Kbytes free
==========================================================
Boot:
Filename                                Size        Created
*boot0:bload                            746 KB      May 09 2004, 19:02:16
*boot0:mx030000.020                     8182 KB     May 09 2004, 18:58:16
boot1:mx030000.020                      8197 KB     May 21 2004, 18:01:02
Boot0: Total:       8928 Kbytes used, 3312 Kbytes free
Boot1: Total:       8197 Kbytes used, 4060 Kbytes free
==========================================================
temporary files:
Filename                                Size        Created
Total:      0 bytes used, 93537 Kbytes free
```

**See Also:**
- dir
- rmdir

# reset system

Restarts a switch and reboots the software.

**Syntax: reset system [force]**

**force***:* Immediately restarts the system and reboots, without comparing the running configuration to the configuration file.

**Defaults:** None.

**Access:** Enabled.

**Usage:** If you do not use the **force** option, the command first compares the running configuration to the configuration file. If the running configuration and configuration file do not match, MSS does not restart the switch but instead displays a message advising you to either save the configuration changes or use the **force** option.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command restarts a switch that does not have any unsaved configuration changes:

```
DWS-1008# reset system
This will reset the entire system. Are you sure (y/n)y
```

The following commands attempt to restart a switch with a running configuration that has unsaved changes, and then force the switch to restart:

```
DWS-1008# reset system
error: Cannot reset, due to unsaved configuration changes. Use “reset system force” to override.

DWS-1008# reset system force
..... rebooting .....
```

**See Also:**
- save config
- show boot
- show version

# restore

Unzips a system archive created by the **backup** command and copies the files from the archive onto the switch.

**Syntax: restore system [tftp:/***ip-addr/***]***filename* **[all | critical] [force]**

| | |
|---|---|
| **[tftp:/***ip-addr/***]***filename* | Name of the archive file to load. The archive can be located in the switch’s nonvolatile storage or on a TFTP server. |
| **all** | Restores system files ***and*** the user files from the archive. |
| **critical** | Restores system files only, including the configuration file used when booting, and certificate files. |
| **force** | Replaces files on the switch with those in the archive, even if the switch is not the same as the one from which the archive was created.<br>**CAUTION:** Do not use this option unless advised to do so by D-Link tech support. If you restore one switch’s system files onto another switch, you must generate new key pairs and certificates on the switch. |

**Defaults:** The default is **critical**.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** If a file in the archive has a counterpart on the switch, the archive version of the file replaces the file on the switch. The **restore** command does not delete files that do not have counterparts in the archive. For example, the command does not completely replace the user files area. Instead, files in the archive are added to the user files area. A file in the user area is replaced only if the archive contains a file with the same name.

**Note:** If the archive's files cannot fit on the switch, the restore operation fails. D-Link recommends deleting unneeded image files before creating or restoring an archive.

The **backup** command stores the MAC address of the switch in the archive. By default, the **restore** command works only if the MAC address in the archive matches the MAC address of the switch where the **restore** command is entered. The **force** option overrides this restriction and allows you to unpack one switch's archive onto another switch.

**Caution:** Do not use the **force** option unless you are certain you want to replace the switch's files with files from another switch. If you restore one switch's system files onto another switch, you must generate new key pairs and certificates on the switch.
If the configuration running on the switch is different from the one in the archive or you renamed the configuration file, and you want to retain changes that were made after the archive was created, see the "Managing System Files" chapter of the D-Link Mobility System Software Configuration Guide.

**Examples:** The following command restores system-critical files on a switch, from archive *sysa_bak*:

```
DWS-1008# restore system tftp:/10.10.20.9/sysa_bak
success: received 11908 bytes in 0.150 seconds [ 79386 bytes/sec]

success: restore complete.
```

**See Also:**
• backup

# rmdir

Removes a subdirectory from nonvolatile storage.

**Syntax: rmdir [***subdirname***]**

| | |
|---|---|
| *subdirname* | Subdirectory name. Specify between 1 and 32 alphanumeric characters, with no spaces. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** MSS does not allow the subdirectory to be removed unless it is empty. Delete all files from the subdirectory before attempting to remove it.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following example removes subdirectory *corp2*:

```
DWS-1008# rmdir corp2
success: change accepted.
```

**See Also:**
- dir
- mkdir

# save config

Saves the running configuration to a configuration file.

**Syntax: save config [***filename***]**

| | |
|---|---|
| *filename* | Name of the configuration file. Specify between 1 and 128 alphanumeric characters, with no spaces.<br>To save the file in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: **backup_configs/config_c**. |

**Defaults:** By default, MSS saves the running configuration as the configuration filename used during the last reboot.

**Access:** Enabled.

**Usage:** If you do not specify a filename, MSS replaces the configuration file loaded during the most recent reboot. To display the filename of the configuration file MSS loaded during the most recent reboot, use the **show boot** command.

The command completely replaces the specified configuration file with the running configuration.

**Examples:** The following command saves the running configuration to the configuration file loaded during the most recent reboot. In this example, the filename used during the most recent reboot is *configuration*.

```
DWS-1008# save config
Configuration saved to configuration.
```

The following command saves the running configuration to a file named *testconfig1*:

```
DWS-1008# save config testconfig1
Configuration saved to testconfig1.
```

**See Also:**
- load config
- show boot
- show config


Download from Www.Somanuals.com. All Manuals Search And Download.

# set boot backup-configuration

Specifies the name of a backup configuration file to be used in the event that MSS cannot read the switch's configuration file at boot time.

**Syntax: set boot backup-configuration** *filename*

| | |
|---|---|
| *filename* | Name of the file to use as a backup configuration file if MSS cannot read the switch's configuration file. |

**Defaults:** By default, there is no backup configuration file.

**Access:** Enabled.

**Examples:** The following command specifies a file called backup.cfg as the backup configuration file on the switch:

```
DWS-1008# set boot backup-configuration backup.cfg
success: backup boot config filename set.
```

**See Also:**
- clear boot backup-configuration
- show boot

# set boot configuration-file

Changes the configuration file to load after rebooting.

**Syntax: set boot configuration-file** *filename*

| | |
|---|---|
| *filename* | Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.<br><br>To load the file from a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: **backup_configs/config_c**. |

**Defaults:** The default configuration filename is *configuration*.

**Access:** Enabled.

**Usage**: The file must be located in the switch's nonvolatile storage.

**Examples:** The following command sets the boot configuration file to *testconfig1*:

```
DWS-1008# set boot configuration-file testconfig1
success: boot config set.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set boot partition

Specifies the boot partition in which to look for the system image file following the next system reset, software reload, or power cycle.

**Syntax: set boot partition {boot0 | boot1}**

**boot0** Boot partition 0.

**boot1** Boot partition 1.

**Defaults:** By default, a switch uses the same boot partition for the next software reload that was used to boot the currently running image.

**Access:** Enabled.

**Usage:** To determine the boot partition that was used to load the currently running software image, use the **dir** command.

**Examples:** The following command sets the boot partition for the next software reload to partition 1:

```
DWS-1008# set boot partition boot1
success: Boot partition set to boot1.
```

# show boot

Displays the system image and configuration filenames used after the last reboot and configured for use after the next reboot.

**Syntax: show boot**

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command shows the boot information for a switch:

```
DWS-1008# show boot
Configured boot version:          4.1.0.65
Configured boot image:            boot1:mx040100.020
Configured boot configuration:    file:configuration
Backup boot configuration:        file:backup.cfg
Booted version:                   4.1.0.65
Booted image:                     boot1:mx040100.020
Booted configuration:             file:configuration
Product model:                    switch
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields in the show boot output.

| Field | Description |
|---|---|
| Configured boot version | Software version the switch will run next time the software is rebooted. |
| Configured boot image | Boot partition and image filename MSS will use to boot next time the software is rebooted. |
| Configured boot configuration | Configuration filename MSS will use to boot next time the software is rebooted. |
| Backup boot configuration | The name of the configuration file to be used in the event that MSS cannot read the configured boot configuration file next time the software is rebooted. |
| Booted version | Software version the switch is running. |
| Booted image | Boot partition and image filename MSS used the last time the software was rebooted. MSS is running this software image. |
| Booted configuration | Configuration filename MSS used to load the configuration the last time the software was rebooted. |

**See Also:**
- clear boot config
- reset system
- set boot configuration-file

# show config

Displays the configuration running on the switch.

**Syntax: show config [area** *area***] [all]**

**area** *area*

Configuration area. You can specify one of the following:
- **aaa**
- **acls**
- **ap**
- **arp**
- **eapol**
- **httpd**
- **ip**
- **ip-config**
- **l2acl**
- **log**
- **mobility-domain**
- **network-domain**
- **ntp**
- **portconfig**
- **port-group**
- **qos**
- **radio-profile**
- **rfdetect**
- **service-profile**
- **sm**
- **snmp**
- **snoop**


Download from Www.Somanuals.com. All Manuals Search And Download.

- **spantree**
- **system**
- **trace**
- **vlan**
- **vlan-fdb**

If you do not specify a configuration area, nondefault information for all areas is displayed.

**all** Includes configuration items that are set to their default values.

**Defaults:** None.

**Access:** Enabled.

**Usage:** If you do not use one of the optional parameters, configuration commands that set nondefault values are displayed for all configuration areas. If you specify an area, commands are displayed for that area only. If you use the **all** option, the display also includes commands for configuration items that are set to their default values.

**Examples:** The following command shows configuration information for VLANs:

```
DWS-1008# show config area vlan
# Configuration nvgen'd at 2004-5-21 19:36:48
# Image 3.0.0
# Model switch
# Last change occurred at 2004-5-21 18:20:50
set vlan 1 port 1
```

**See Also:**
- load config
- save config

# show version

Displays software and hardware version information for a switch and, optionally, for any attached access points.

**Syntax: show version [details]**

**details** Includes additional software build information and information about the AP access points configured on the switch.

**Defaults:** None.

**Access:** All.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command displays version information for a switch:

```
DWS-1008# show version
        Mobility System Software, Version: 4.1.0 QA 67
        Copyright (c) 2002, 2003, 2004, 2005 D-Link, Inc. All rights reserved.
Build Information: (build#67) TOP 2005-07-21 04:41:00
Model:          DWS-1008
Hardware
        Mainboard:      version 24 ; revision 3 ; FPGA version 24
        PoE board:      version 1 ; FPGA version 6
Serial number      0321300013
Flash:          4.1.0.14  - md0a
Kernel:         3.0.0#20: Fri May 20 17:43:51 PDT 2005
BootLoader:       4.10 / 4.1.0
```

The following command displays additional software build information and access point information:

```
DWS-1008# show version details
        Mobility System Software, Version: 4.1.0 QA 67
        Copyright (c) 2002, 2003, 2004, 2005 D-Link, Inc. All rights reserved.
Build Information: (build#67) TOP 2005-07-21 04:41:00
        Label:          4.1.0.67_072105_MX20
        Build Suffix:     -d-O1
        Model:          DWS-1008
        Hardware
                Mainboard:      version 24 ; revision 3 ; FPGA version 24
                CPU Model:      750 (Revision 3.1)
                PoE board:      version 1 ; FPGA version 6
        Serial number      0321300013
        Flash:          4.1.0.14  - md0a
        Kernel:         3.0.0#20: Fri May 20 17:43:51 PDT 2005
        BootLoader:       4.10 / 4.1.0

        Port/DAP      AP Model     Serial #            Versions
        --------      ----------   --------------      ------------------------
        11  /-        AP-352       0424902948          H/W  : A
                                                       F/W1 : 5.6
                                                       F/W2 : 5.6
                                                       S/W    : 4.1.0.67_072105_0432__AP
                                                       BOOT S/W : 4.0.3.15_062705_0107__AP
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields in the **show version** output.

| Field | Description |
|---|---|
| Build Information | Factory timestamp of the image file. |
| Label | Software version and build date. |
| Build Suffix | Build suffix. |
| Model | Build model. |
| Hardware | Version information for the switch's motherboard and Power over Ethernet (PoE) board. |
| Serial number | Serial number of the switch. |
| Flash | Flash memory version. |
| Kernel | Kernel version. |
| BootLoader | Boot code version. |
| Port/DAP | Port number connected to an access point. |
| AP Model | AP model number. |
| Serial # | AP serial number. |
| Versions | AP hardware, firmware, and software versions. |

# uninstall soda agent

Removes the contents of a directory containing SODA agent files.

**Syntax: uninstall soda agent agent-directory** *directory*

*directory* Directory on the switch where SODA agent files are to be removed.

**Defaults:** None.

**Access:** Enabled.

**Usage:** Use this command to remove a SODA agent directory and all of its contents. All files in the specified directory are removed. The command removes the directory and its contents, regardless of whether it contains SODA agent files.

**Examples:** The following command removes the directory sp1 and all of its contents:

```
DWS-1008# uninstall soda agent agent-directory sp1
This will delete all files in agent-directory, do you wish to continue? (y|n) [n]y
```

**See Also:**
- install soda agent
- set service-profile soda mode


Download from Www.Somanuals.com. All Manuals Search And Download.

# Access Point Commands

Use DWL-8220AP access point commands to configure and manage DWL-8220AP access points. Be sure to do the following before using the commands:

- Define the country-specific IEEE 802.11 regulations on the DWS-1008 switch.
- Install the DWL-8220AP access point and connect it to a port on the switch.
- Configure an DWL-8220AP access port (for a directly connected AP) or a Distributed AP).

**Caution:** Changing the system country code after DWL-8220AP configuration disables DWL-8220AP access points and deletes their configuration. If you change the country code on a switch, you must reconfigure all DWL-8220AP access points.

## clear {ap | dap} radio

Disables an DWL-8220AP radio and resets it to its factory default settings.

**Syntax: clear {ap** *port-list* **| dap** *dap-num***} radio {1 | 2 | all}**

| | |
|---|---|
| **ap** *port-list* | List of ports connected to the DWL-8220AP access point(s) on which to reset a radio. |
| **dap** *dap-num* | Number of a Distributed AP on which to reset a radio. |
| **radio 1** | Radio 1 of the DWL-8220AP. |
| **radio 2** | Radio 2 of the DWL-8220AP. |
| **radio all** | All radios on the DWL-8220AP. |

**Defaults:** The clear ap radio command resets the radio to the default settings.

**Usage:** When you clear a radio, MSS performs the following actions:

- Clears the transmit power, channel, and external antenna setting from the radio.
- Removes the radio from its radio profile and places the radio in the default radio profile.

This command does not affect the PoE (Power over Ethernet) setting.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples** The following command disables and resets radio 2 on the DWL-8220AP access point connected to port 3:

```
DWS-1008# clear ap 3 radio 2
```

# clear dap boot-configuration

Removes the static IP address configuration for a Distributed AP.

**Syntax: clear dap boot-configuration** *dap-num*

**dap** *dap-num* Number of the Distributed AP for which you are clearing static IP information.

**Defaults:** None.

**Access:** Enabled

**Usage:** When the static IP configuration is cleared for a Distributed AP, the next time the Distributed AP is rebooted, it uses the standard boot process.

**Examples:** The following command clears the static IP address configuration for Distributed AP 1.

```
DWS-1008# clear dap 1 boot-configuration
This will clear specified DAP devices. Would you like to continue? (y/n)
[n]y
success: change accepted.
```

**See Also:**

- set dap boot-ip
- set dap boot-switch
- set dap boot-vlan
- show dap boot-configuration


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear radio-profile

Removes a radio profile or resets one of the profile's parameters to its default value.

**Syntax: clear radio-profile** *name [parameter]*

| | |
|---|---|
| *name* | Radio profile name. |
| *parameter* | Radio profile parameter:<br>• beacon-interval<br>• countermeasures<br>• dtim-interval<br>• frag-threshold<br>• max-rx-lifetime<br>• max-tx-lifetime<br>• preamble-length<br>• rts-threshold<br>• service-profile<br>(For information about these parameters, see the set radio-profile commands that use them.) |

**Defaults** If you reset an individual parameter, the parameter is returned to it's default value.

**Access:** Enabled

**Usage:** If you specify a parameter, the setting for the parameter is reset to its default value. The settings of the other parameters are unchanged and the radio profile remains in the configuration. If you do not specify a parameter, the entire radio profile is deleted from the configuration. All radios that use this profile must be disabled before you can delete the profile.

**Examples:** The following commands disable the radios that are using radio profile *rp1* and reset the **beaconed-interval** parameter to its default value:

```
DWS-1008# set radio-profile rp1 mode disable

DWS-1008# clear radio-profile rp1 beacon-interval
success: change accepted.
```

The following commands disable the radios that are using radio profile rptest and remove the profile:

```
DWS-1008# set radio-profile rptest mode disable

DWS-1008# clear radio-profile rptest
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

**See Also:**

- set {ap | dap} radio radio-profile
- set radio-profile mode
- show {ap | dap} config
- show radio-profile

# clear service-profile

Removes a service profile or resets one of the profile's parameters to its default value.

**Syntax: clear service-profile** *name*
**[soda {agent-directory | failure-page | remediation-acl | success-page | logout-page}]**

*name* Service profile name.

**soda agent-directory** Resets the directory for Sygate On-Demand (SODA) agent files to the default directory. By default, the directory name for SODA agent files is the same as the service profile name.

**soda failure-page** Resets the page that is loaded when a client fails the checks performed by the SODA agent. By default, the page is generated dynamically.

**soda remediation-acl** Disables use of the specified remediation ACL for the service profile. When no remediation ACL is specified, a client is disconnected form the network when it fails SODA agent checks.

**soda success-page** Resets the page that is loaded when a client passes the checks performed by the SODA agent. By default, the page is generated dynamically.

**soda logout-page** Resets the page that is loaded when a client logs out of the network. By default, the client is disconnected from the network without a page being loaded.

**Defaults:** None

**Access:** Enabled

**Usage:** If the service profile is mapped to a radio profile, you must remove it from the radio profile first. (After disabling all radios that use the radio profile, use the **clear radio-profile** *name* **service-profile** *name* command.)


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following commands disable the radios that are using radio profile *rp6*, remove service-profile *svcprof6* from *rp6*, then clear *svcprof6* from the configuration.

```
DWS-1008# set radio-profile rp6 mode disable

DWS-1008# clear radio-profile rp6 service-profile svcprof6
success: change accepted.

DWS-1008# clear service-profile svcprof6
success: change accepted.
```

**See Also:**
- clear radio-profile
- set radio-profile mode
- show service-profile

# reset {ap | dap}

Restarts an access point.

**Syntax: reset {ap** *port-list* **| dap** *dap-num***}**

**ap** *port-list* List of ports connected to the access points to restart.

**dap** *dap-num* Number of a Distributed AP to reset.

**Defaults:** None.

**Access:** Enabled

**Usage:** When you enter this command, the AP drops all sessions and reboots.

**Examples:** The following command resets the AP on port 4:

```
DWS-1008# reset ap 4
This will reset specified AP devices. Would you like to continue? (y/n)y
success: rebooting ap attached to port 4
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set dap auto

Creates a profile for automatic configuration of Distributed APs.

**Syntax: set dap auto**

**Defaults:** None.

**Access:** Enabled.

The following Table lists the configurable profile parameters and their defaults. The only parameter that requires configuration is the profile mode. The profile is disabled by default. To use the profile to configure Distributed APs, you must enable the profile using the **set dap auto mode enable** command.

The profile uses the *default* radio profile by default. You can change the profile using the **set dap auto radio radio-profile** command. You can use **set dap auto** commands to change settings for the parameters listed in the following table. (The commands are listed in the "See Also" section.)

| Parameter | Default Value |
|---|---|
| **AP Parameters** | |
| bias | high |
| blink<br>(Not shown in show dap config output) | disable |
| force-image-download | None. |
| group (load balancing) | none |
| mode | disabled |
| persistent | none |
| upgrade-firmware<br>(boot-download-enable) | enable (YES) |
| **Radio Parameters** | |
| radio num auto-tune max-power | default |
| radio num mode | enabled |
| radio num radio-profile | default |
| radiotype | 11g (or 11b for country codes where 802.11g is not allowed) |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command creates a profile for automatic Distributed AP configuration:

```
DWS-1008# set dap auto
success: change accepted.
```

**See Also:**
- set dap auto mode
- set dap auto persistent
- set dap auto radiotype
- set {ap | dap} bias
- set {ap | dap} blink
- set {ap | dap} group
- set {ap | dap} radio auto-tune max-power
- set {ap | dap} radio mode
- set {ap | dap} radio radio-profile
- set {ap | dap} upgrade-firmware

# set dap auto mode

Enables an DWS-1008's profile for automatic Distributed AP configuration.

**Syntax: set dap auto mode {enable | disable}**

**enable** Enables the AP configuration profile.

**disable** Disables the AP configuration profile.

**Defaults:** The AP configuration profile is disabled by default.

**Access:** Enabled

**Usage:** You must use the set dap auto command to create the profile before you can enable it.

**Examples:** The following command enables the profile for automatic Distributed AP configuration:

```
DWS-1008# set dap auto mode enable
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set dap auto persistent

Converts a temporary AP configuration created by the AP configuration profile into a persistent AP configuration on the DWS-1008.

**Syntax: set dap auto persistent [***dap-num* **| all]**

| | |
|---|---|
| ***dap-num*** | Converts the configuration of the Distributed AP that has the specified connection number into a permanent configuration. |
| **all** | Converts the configurations of all Auto-APs being managed by the switch into permanent configurations. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** To display the Distributed AP numbers assigned to Auto-APs, use the s**how dap status auto** command.

**Examples:** The following command converts the configuration of Auto-AP 10 into a permanent configuration:

```
DWS-1008# set dap auto persistent 10
success: change accepted
```

**See Also:**
- set dap auto
- set dap auto mode
- set dap auto radiotype

# set dap auto radiotype

Sets the radio type for single-AP radios that use the AP configuration profile.

**Syntax: set dap auto [radiotype {11a | 11b| 11g}]**

| | |
|---|---|
| **radiotype 11a \| 11b \| 11g** | Radio type:<br>• 11g - 802.11a<br>• 11a - 802.11b<br>• 11g - 802.11g |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** The default radio type for the DWL-8220AP is 802.11g.

**Access:** Enabled

**Examples:** The following command sets the radio type to 802.11b:

```
DWS-1008# set dap auto radiotype 11b
success: change accepted.
```

**See Also:**
- set dap auto
- set dap auto mode
- set dap auto persistent

# set {ap | dap} bias

Changes the bias for an AP. Bias is the priority of one DWS-1008 switch over other DWS-1008 switches for booting and configuring the AP.

**Syntax: set {ap** *port-list* **| dap {***dap-num* **| auto}} bias {high | low}**

| | |
|---|---|
| **ap** *port-list* | List of ports on which to change the bias for directly connected APs. |
| **dap** *dap-num* | Number of a Distributed AP for which to change the bias. |
| **dap auto** | Configures bias for the AP configuration profile. |
| **high** | High bias. |
| **low** | Low bias. |

**Defaults:** The default bias is high.

**Access:** Enabled

**Usage:** High bias is preferred over low bias. Bias applies only to DWS-1008 switches that are indirectly attached to the AP through an intermediate Layer 2 or Layer 3 network. An AP always attempts to boot on AP port 1 first, and if a DWS-1008 is directly attached on AP port 1, the AP always boots from it.


Download from Www.Somanuals.com. All Manuals Search And Download.

If AP port 1 is indirectly connected to DWS-1008 switches through the network, the AP boots from the switch with the high bias for the AP. If the bias for all connections is the same, the AP selects the switch that has the greatest capacity to add more active APs. For example, if an AP is dual homed to two DWS-1008 switches, and one of the switches has 50 active APs while the other switch has 60 active APs, the new AP selects the switch that has only 50 active APs.

If the boot request on AP port 1 fails, the AP attempts to boot over its port 2, using the same process described above.

AP selection of an DWS-1008 is static. After an AP selects a DWS-1008 switch to boot from, the AP continues to use that switch for its active data link even if another switch configured with high bias for the AP becomes available.

The following command changes the bias for a Distributed AP to low:

```
DWS-1008# set dap 1 bias low
success: change accepted.
```

**See Also:**
• show {ap | dap} config

# set {ap | dap} blink

Enables or disables LED blink mode on a DWL-8220AP access point to make it easy to identify. When blink mode is enabled on DWL-8220AP-xxx models, the health and radio LEDs alternately blink green and amber. By default, blink mode is disabled.

**Syntax: set {ap** *port-list* **| dap {***dap-num* **| auto}} blink {enable | disable}**

| | |
|---|---|
| **ap** *port-list* | List of ports connected to the AP access points on which to turn blink mode on or off. |
| **dap** *dap-num* | Number of a Distributed AP on which to turn blink mode on or off. |
| **dap auto** | Configures blink mode for the AP configuration profile. |
| **enable** | Enables blink mode. |
| **disable** | Disables blink mode. |

**Defaults:** LED blink mode is disabled by default.

**Access:** Enabled

**Usage:** Changing the LED blink mode does not alter operation of the DWL-8220AP access point. Only the behavior of the LEDs is affected.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command enables LED blink mode on the access points connected to ports 3 and 4:

```
DWS-1008# set ap 3-4 blink enable
success: change accepted.
```

# set dap boot-ip

Specifies static IP address information for a Distributed AP.

**Syntax: set dap** *dap-num* **boot-ip ip** *ip-addr* **netmask** *mask-addr* **gateway** *gateway-addr* **[mode {enable | disable}]**

**Syntax: set dap** dap-num **boot-ip mode {enable | disable}**

| | |
|---|---|
| **dap** *dap-num* | Number of the Distributed AP for which you are specifying static IP information. |
| **ip** *ip-addr* | The IP address to be assigned to the AP, in dotted decimal notation (for example, 10.10.10.10). |
| **netmask** *mask-addr* | The subnet mask, in dotted decimal notation (for example, 255.255.255.0). |
| **gateway** *gateway-addr* | The IP address of the next-hop router, in dotted decimal notation. |
| **mode {enable \| disable}** | Enables or disables the static IP address for the AP. |

**Defaults:** By default APs use DHCP to obtain an IP address, rather than a using a manually assigned IP address.

**Access:** Enabled

**Usage:** Normally, Distributed APs use DHCP to obtain IP address information. In some installations, DHCP may not be available. In this case, you can assign static IP address information to the AP, including the AP's IP address and netmask, and default gateway.

If the manually assigned IP information is incorrect, the AP uses DHCP to obtain its IP address.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command configures Distributed AP 1 to use IP address 172.16.0.42 with a 24-bit netmask, and use 172.16.0.20 as its default gateway:

DWS-1008# **set dap 1 boot-ip ip 172.16.0.42 netmask 255.255.255.0 gateway 172.16.0.20 mode enable**
success: change accepted.

**See Also:**
- clear dap boot-configuration
- set dap boot-switch
- set dap boot-vlan
- show dap boot-configuration

# set dap boot-switch

Specifies the DWS-1008 a Distributed AP contacts and attempts to use as its boot device.

**Syntax: set dap** *dap-num* **boot-switch [switch-ip** *ip-addr***] [name** *name* **dns** *ip-addr***] [mode {enable | disable}]**

| | |
|---|---|
| **dap** *dap-num* | Number of the Distributed AP for which you are specifying static IP information. |
| **switch ip** *ip-addr* | The IP address of the DWS-1008 the Distributed AP should boot from. |
| **name** *name* | The fully qualified domain name of the DWS-1008 the Distributed AP should boot from. When both a name and a switch-ip are specified, the AP uses the name. |
| **dns** *ip-addr* | The IP address of the DNS server used to resolve the specified name of the DWS-1008. |
| **mode {enable \| disable}** | Enables or disables the AP using the specified boot device. |

**Defaults:** By default APs use the process described in “Default AP Boot Process”, in the D-Link Mobility System Software Configuration Guide to boot from a DWS-1008, instead of using a manually specified DWS-1008.

**Access:** Enabled

**Usage:** When you specify a boot switch for a distributed AP to boot from, it boots using the process described in “AP Boot Process Using Static IP Configuration”, in the D-Link Mobility System Software Configuration Guide.


Download from Www.Somanuals.com. All Manuals Search And Download.

When a static IP address is specified for a Distributed AP, there is no preconfigured DNS information or DNS name for the DWS-1008 the Distributed AP attempts to use as its boot device. If you configure a static IP address for a Distributed AP, but do not specify a boot device, then the DWS-1008 switch must be reachable via subnet broadcast.

**Examples:** The following command configures Distributed AP 1 to use the DWS switch with address 172.16.0.21 as its boot device.

```
DWS-1008# set dap 1 boot-switch switch-ip 172.16.0.21 mode enable
success: change accepted.
```

The following command configures Distributed AP 1 to use the DWS switch with the name dws2 as its boot device. The DNS server at 172.16.0.1 is used to resolve the name of the DWS switch.

```
DWS-1008# set dap 1 boot-switch name dws2 dns 172.16.0.1 mode enable
success: change accepted.
```

**See Also:**
- clear dap boot-configuration
- set dap boot-ip
- set dap boot-vlan
- show dap boot-configuration

# set dap boot-switch

Specifies 802.1Q VLAN tagging information for a Distributed AP.

**Syntax: set dap** *dap-num* **boot-vlan vlan-tag** *tag-value* **[mode {enable | disable}]**

**Syntax: set dap dap-num boot-vlan mode {enable | disable}**

| | |
|---|---|
| **dap** *dap-num* | Number of the Distributed AP for which you are specifying VLAN information. |
| **vlan-tag** *tag-value* | The VLAN tag value. You can specify a number from 1 – 4095. |
| **mode {enable \| disable}** | Enables or disables use of the specified VLAN tag on the Distributed AP. |

**Defaults:** None.

**Access:** Enabled


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** When this command is configured, all Ethernet frames emitted from the Distributed AP are formatted with an 802.1Q tag with a specified VLAN number. Frames sent to the Distributed AP that are not tagged with this value are ignored.

**Examples:** The following command configures Distributed AP 1 to use VLAN tag 100:

```
DWS-1008# set dap 1 boot-vlan vlan-tag 100 mode enable
success: change accepted.
```

**See Also:**
- clear dap boot-configuration
- set dap boot-ip
- set dap boot-switch
- show dap boot-configuration

# set {ap | dap} contact

Specifies contact information for an AP.

**Syntax: set {ap** *port-list* **| dap {***dap-num***} contact** *string*

| | |
|---|---|
| **ap** *port-list* | List of ports on which to specify contact information for directly connected APs. |
| **dap** *dap-num* | Number of a Distributed AP for which to specify contact information. |
| **contact** *string* | Contact information for the AP. If the contact information includes spaces, enclose the string in quotes. |

**Defaults:** None.

**Access:** Enabled

**Usage:** Use this command to specify an individual or department to contact for information or maintenance on the AP.

**Examples:** The following command specifies the contact person for AP 7 as *Bob the IT guy*.

```
DWS-1008# set ap 7 contact 'Bob the IT guy'
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set dap fingerprint

Verifies an AP's fingerprint on an DWS-1008. If AP-DWS security is required by an DWS-1008, an AP can establish a management session with the switch only if you have verified the AP's identity by verifying its fingerprint on the switch.

**Syntax: set dap** *dap-num* **fingerprint** *hex*

| | |
|---|---|
| **dap** *dap-num* | Number of the Distributed AP whose fingerprint you are verifying. |
| *hex* | The 16-digit hexadecimal number of the fingerprint. Use a colon between each digit. Make sure the fingerprint you enter matches the fingerprint used by the AP. |

**Defaults:** None.

**Access:** Enabled

**Usage:** APs are configured with an encryption key pair at the factory. The fingerprint for the public key is displayed on a label on the back of the AP, in the following format:

```
RSA
aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa
```

If an AP is already installed and operating, you can use the show dap status command to display the fingerprint. The show dap config command lists an AP's fingerprint only if the fingerprint has been verified in MSS. If the fingerprint has not been verified, the fingerprint information in the command output is blank.

**Examples:** The following example verifies the fingerprint for Distributed AP 8:

```
DWS-1008# set dap 8 fingerprint b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
success: change accepted.
```

**See Also:**
- set dap security
- show {ap | dap} config
- show {ap | dap} status


Download from Www.Somanuals.com. All Manuals Search And Download.

# set {ap | dap} force-image-download

Configures an AP to download its software image from the DWS-1008 instead of loading the image that is locally stored on the AP.

**Syntax: set {ap** *port-list* **| dap {***dap-num* **| auto}} force-image-download {enable | disable}**

| | |
|---|---|
| **ap** *port-list* | List of AP access ports. |
| **dap** *dap-num* | Number of a Distributed AP. |
| **dap auto** | Configures forced image download for the AP configuration profile. |
| **force-image-download enable** | Enables forced image download. |
| **force-image-download disable** | Disables forced image download. |

**Defaults:** Forced image download is disabled by default.

**Access:** Enabled

**Usage:** A change to the forced image download option takes place the next time the AP is restarted. Even when forced image download is disabled (the default), the AP still checks with the DWS-1008 to verify that the AP has the latest image.

**Examples:** The following command enables forced image download on Distributed AP 69:

```
DWS-1008# set dap 69 force-image-download enable
success: change accepted.
```

**See Also:**
• show {ap | dap} config


Download from Www.Somanuals.com. All Manuals Search And Download.

# set {ap | dap} group

Configures a named group of AP access points. MSS automatically load balances sessions among the access points in a group. To balance the sessions, MSS rejects an association request for an access point's radio if that radio has at least four more active sessions than the radio of the same type with the least number of active sessions within the group.

**Syntax: set {ap** *port-list* **| dap {***dap-num* **| auto}} group** *name*

| | |
|---|---|
| **ap** *port-list* | List of AP access ports to add to the group. |
| **dap** *dap-num* | Number of a Distributed AP to add to the group. |
| **dap auto** | Configures an AP group for the AP configuration profile. |
| *name* | AP access point group name of up to 16 alphanumeric characters, with no spaces. |

**Defaults:** AP access points are not grouped by default.

**Access:** Enabled

**Usage:** You can assign any subset or all of the access points connected to a DWS-1008 to a group on that switch. All access points in a group must be connected to the same DWS-1008.

If you use the name none, spelled in any combination of capital or lowercase letters, the specified access point is cleared from all AP groups.

**Examples:** The following command configures an DWL-8220AP access point group named *loadbalance1* that contains the access points on ports 1, 4, and 7:

```
DWS-1008# set ap 1,4,7 group loadbalance1
success: change accepted.
```

**See Also:**
- show {ap | dap} config
- show {ap | dap} group


Download from Www.Somanuals.com. All Manuals Search And Download.

# set {ap | dap} location

Specifies location information for an AP.

**Syntax: set {ap** *port-list* **| dap {***dap-num***} location** *string*

| | |
|---|---|
| **ap** *port-list* | List of ports on which to specify location information for directly connected APs. |
| **dap** *dap-num* | Number of a Distributed AP for which to specify location information. |
| **location** *string* | Location information for the AP. If the location information includes spaces, enclose the string in quotes. |

**Defaults:** None.

**Access:** Enabled

**Usage:** Use this command to specify information about the location of the AP.

**Examples:** The following command specifies the location of AP 7 as The conference room.

```
DWS-1008# set ap 7 location 'The conference room'
success: change accepted.
```

**See Also:**
- show {ap | dap} config
- set {ap | dap} contact


Download from Www.Somanuals.com. All Manuals Search And Download.

# set {ap | dap} name

Changes an AP name.

**Syntax: set {ap** *port-list* **| dap** *dap-num***} name** *name*

| | |
|---|---|
| **ap** *port-list* | List of ports connected to the AP access point to rename. |
| **dap** *dap-num* | Number of a Distributed AP to rename. |
| *name* | Alphanumeric string of up to 16 characters, with no spaces. |

**Defaults:** The default name of a directly attached AP is based on the port number of the AP access port attached to the AP. For example, the default name for an AP on AP access port 1 is AP01. The default name of a Distributed AP is based on the number you assign to it when you configure the connection. For example, the default name for Distributed AP 1 is DAP01.

**Access:** Enabled

**Examples:** The following command changes the name of the AP on port 1 to *techpubs*:

```
DWS-1008# set ap 1 name techpubs
success: change accepted.
```

**See Also:**
• show {ap | dap} config

# set {ap | dap} radio antenna-location

Specifies the location (indoors or outdoors) of an external antenna. Use this command to ensure that the proper set of channels is available on the radio. In some cases, the set of valid channels for a radio differs depending on whether the antenna is located indoors or outdoors.

**Syntax: set {ap *port-list* | dap *dap-num*} antenna-location {indoors | outdoors}**

| | |
|---|---|
| **ap** *port-list* | List of ports connected to the AP access point to rename. |
| **dap** *dap-num* | Number of a Distributed AP to rename. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**indoors** Specifies that the external antenna is installed inside the building.

**outdoors** Specifies that the external antenna is installed outdoors.

**Defaults:** The default antenna location is indoors.

**Access:** Enabled

**Examples:** The following command sets the antenna location for radio 1 on Distributed AP 22 to **outdoors**:

```
DWS-1008# set dap 22 radio 1 antenna-location outdoors
success: change accepted.
```

**See Also:**
• set {ap | dap} radio antennatype

# set {ap | dap} radio antennatype

Sets the model number for an external antenna.

**Syntax: set {ap** *port-list* **| dap** *dap-num***} radio {1 antennatype ANT1060 | ANT1120 | ANT1180 | internal} | {2 antennatype ANT5060 | ANT5120 | ANT5180 | internal}**

**ap** *port-list* List of ports connected to the DWL-8220AP access points on which to set the channel.

**dap** *dap-num* Number of a Distributed AP on which to set the channel.

**radio 1** Radio 1 of the DWL-8220AP.

**radio 2** Radio 2 of the DWL-8220AP.

**radio 1 antennatype** 802.11b/g external antenna models:
- ANT1060 - 60° 802.11b/g antenna
- ANT1120 - 120° 802.11b/g antenna
- ANT1180 - 180° 802.11b/g antenna
- internal - Uses the internal antenna instead

**radio 2 antennatype** 802.11a external antenna models:
- ANT5060 - 60° 802.11a antenna
- ANT5120 - 120° 802.11a antenna
- ANT5180 - 180° 802.11a antenna
- internal - Uses the internal antenna instead


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** All radios use the internal antenna by default.

**Access:** Enabled

**Examples:** The following command configures the 802.11b/g radio on Distributed AP 1 to use antenna model ANT1060:

```
DWS-1008# set dap 1 radio 1 antennatype ANT1060
success: change accepted.
```

**See Also:**
• show {ap | dap} config

# set {ap | dap} radio auto-tune max-power

Sets the maximum power that RF Auto-Tuning can set on a radio.

**Syntax: set {ap** *port-list* **| dap {***dap-num* **| auto}} radio {1 | 2} auto-tune max-power** *power-level*

| | |
|---|---|
| **ap** *port-list* | List of ports connected to the DWL-8220AP access points on which to set the maximum power. |
| **dap** *dap-num* | Number of a Distributed AP on which to set the maximum power. |
| **dap auto** | Sets the maximum power for radios configured by the DWL-8220AP configuration template. |
| **radio 1** | Radio 1 of the DWL-8220AP. |
| **radio 2** | Radio 2 of the DWL-8220AP. |
| **power-level** | Maximum power setting RF Auto-Tuning can assign to the radio, expressed as the number of decibels in relation to 1 milliwatt (dBm). You can specify a value from 1 up to the maximum value allowed for the country of operation. The power-level can be a value from 1 to 20. |

**Defaults:** The default maximum power setting that RF Auto-Tuning can set on a radio is the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Example:** The following command sets the maximum power that RF Auto-Tuning can set on radio 1 on the DWL-8220AP access point on port 5 to 12 dBm.

```
DWS-1008# set ap 5 radio 1 auto-tune max-power 12
success: change accepted.
```

**See Also:**
- set radio-profile auto-tune power-config
- set radio-profile auto-tune power-interval

# set {ap | dap} radio channel

Sets an DWS-8220AP radio's channel.

**Syntax: set {ap** *port-list* **| dap** *dap-num***} radio {1 | 2} channel** *channel-number*

| | |
|---|---|
| **ap** *port-list* | List of ports connected to the DWL-8220AP access points on which to set the channel. |
| **dap** *dap-num* | Number of a Distributed AP on which to set the channel. |
| **radio 1** | Radio 1 of the DWL-8220AP. |
| **radio 2** | Radio 2 of the DWL-8220AP. |
| *channel-number* | Channel number. The valid channel numbers depend on the country of operation. |

**Defaults:** The default channel depends on the radio type:
- The default channel number for 802.11b/g is 6.
- The default channel number for 802.11a is the lowest valid channel number for the country of operation.

**Access:** Enabled.

**Usage:** You can configure a radio's transmit power on the same command line. Use the **tx-power** option. This command is not valid if dynamic channel tuning (RF Auto-Tuning) is enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command configures the channel on the 802.11a radio on the DWL-8220AP access point connected to port 5:

```
DWS-1008# set ap 5 radio 1 channel 36
success: change accepted.
```

The following command configures the channel and transmit power on the 802.11b/g radio on the DWL-8220AP access point connected to port 2:

```
DWS-1008# set ap 2 radio 1 channel 1 tx-power 10
success: change accepted.
```

**See Also:**
- set {ap | dap} radio tx-power
- show {ap | dap} config

# set {ap | dap} radio mode

Enables or disables a radio on a DWL-8220AP access point.

**Syntax: set {ap** *port-list* **| dap {***dap-num* **| auto}} radio {1 | 2} mode {enable | disable}**

| | |
|---|---|
| **ap** *port-list* | List of ports connected to the DWL-8220AP access point(s) on which to turn a radio on or off. |
| **dap** *dap-num* | Number of a Distributed AP on which to turn a radio on or off. |
| **dap auto** | Sets the radio mode for DWL-8220APs managed by the DWL-8220AP configuration template. |
| **radio 1** | Radio 1 of the DWL-8220AP. |
| **radio 2** | Radio 2 of the DWL-8220AP. |
| **enable** | Enables a radio. |
| **disable** | Disables a radio. |

**Defaults:** DWL-8220AP access point radios are disabled by default.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** To enable or disable one or more radios to which a profile is assigned, use the set ap radio radio-profile command. To enable or disable all radios that use a specific radio profile, use the set radio-profile command.

**Examples:** The following command enables radio 1 on the DWL-8220AP access points connected to ports 1 through 5:

```
DWS-1008# set ap 1-5 radio 1 mode enable
success: change accepted.
```

The following command enables radio 2 on ports 1 through 3:

```
DWS-1008# set ap 1-3 radio 2 mode enable
success: change accepted.
```

# set {ap | dap} radio radio-profile

Assigns a radio profile to an DWL-8220AP radio and enables or disables the radio.

**Syntax: set {ap** *port-list* **| dap {***dap-num* **| auto}} radio {1 | 2} radio-profile** *name* **mode {enable | disable}**

| | |
|---|---|
| **ap** *port-list* | List of ports. |
| **dap** *dap-num* | Number of a Distributed AP. |
| **dap auto** | Sets the radio profile for the DWL-8220AP configuration template. |
| **radio 1** | Radio 1 of the DWL-8220AP. |
| **radio 2** | Radio 2 of the DWL-8220AP. |
| **radio-profile** *name* | Radio profile name of up to 16 alphanumeric characters, with no spaces. |
| **mode enable** | Enables radios on the specified ports with the parameter settings in the specified radio profile. |
| **mode disable** | Disables radios on the specified ports. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** When you create a new profile, the radio parameters in the profile are set to their factory default values. To enable or disable all radios that use a specific radio profile, use set radio-profile.

**Access:** Enabled.

**Examples:** The following command enables radio 1 on ports 4 through 6 assigned to radio profile rp1:

```
DWS-1008# set ap 4-6 radio 1 radio-profile rp1 mode enable
success: change accepted.
```

## set {ap | dap} radio tx-power

Sets an DWL-8220AP radio's transmit power.

**Syntax: set {ap** *port-list* **| dap** *dap-num***} radio {1 | 2} tx-power** *power-level*

| | |
|---|---|
| **ap** *port-list* | List of ports connected to the DWL-8220AP access points on which to set the transmit power. |
| **dap** *dap-num* | Number of a Distributed AP on which to set the transmit power. |
| **radio 1** | Radio 1 of the DWL-8220AP. |
| **radio 2** | Radio 2 of the DWL-8220AP. |
| **tx** *power* | Number of decibels in relation to 1 milliwatt (dBm). The power-level valid values depend on the country of operation.<br><br>**Note:** The maximum transmit power you can configure on any D-Link radio is the maximum allowed for the country in which you plan to operate the radio or one of the following values if that value is less than the country maximum: on an 802.11a radio, 11 dBm for channel numbers less than or equal to 64, or 10 dBm for channel numbers greater than 64; on an 802.11b/g radio, 16 dBm for all valid channel numbers for 802.11b, or 14 dBm for all valid channel numbers for 802.11g. |

**Defaults:** The default transmit power on all DWL-8220AP radio types is the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

**Usage:** To enable or disable one or more radios to which a profile is assigned, use the set ap radio radio-profile command. To enable or disable all radios that use a specific radio profile, use the set radio-profile command.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command configures the transmit power on the 802.11a radio on the DWL-8220AP access point connected to port 5:

```
DWS-1008# set ap 5 radio 1 tx-power 10
success: change accepted.
```

The following command configures the channel and transmit power on the 802.11b/g radio on the DWL-8220AP access point connected to port 2:

```
DWS-1008# set ap 2 radio 1 channel 1 tx-power 10
success: change accepted.
```

# set dap security

Sets security requirements for management sessions between a DWS-1008 switch and its Distributed APs. This feature applies to Distributed APs only, not to directly connected DWL-8220APs configured on DWL-8220AP access ports. In addition, DWL-8220AP models DWL-8220AP-101 and DWL-8220AP-122 do not have encryption keys and do not support this feature regardless of how they are connected to the switch.

**Note:** The maximum transmission unit (MTU) for encrypted DWL-8220AP management traffic is 1498 bytes, whereas the MTU for unencrypted management traffic is 1474 bytes. Make sure the devices in the intermediate network between the switch and Distributed AP can support the higher MTU.

**Syntax: set dap security {require | optional | none}**

| | |
|---|---|
| **require** | Require all Distributed APs to have encryption keys that have been confirmed in the CLI by an administrator. |
| **optional** | Allows DWL-8220APs to be managed by the switch even if they do not have encryption keys or their keys have not been configured by an administrator. |
| **none** | Encryption is not used, even for APs that support it. |

**Defaults:** By default, encryption keys are optional.

**Access:** Enabled.

**Usage:** This parameter applies to all Distributed APs managed by the switch. If you change the setting to required, the switch requires Distributed APs to have encryption keys. The switch also requires their fingerprints to be confirmed in MSS. When DWL-8220AP security is required, an


Download from Www.Somanuals.com. All Manuals Search And Download.

AP can establish a management session with the DWS-1008 switch only if its fingerprint has been confirmed by you in MSS.

A change to DWL-8220AP security support does not affect management sessions that are already established. To apply the new setting to an DWL-8220AP, restart the DWL-8220AP.

**Examples:** The following command configures a DWS-1008 to require Distributed APs to have encryption keys:

```
DWS-1008# set dap security require
success: change accepted.
```

**See Also:**
- set dap fingerprint
- show {ap | dap} config
- show {ap | dap} status

# set {ap | dap} upgrade-firmware

Disables or reenables automatic upgrade of a DWL-8220AP access point's boot firmware.

**Syntax: set {ap** *port-list* **| dap {***dap-num* **| auto}} upgrade-firmware {enable | disable}**

| | |
|---|---|
| **ap** *port-list* | List of ports connected to the DWL-8220AP access point(s) on which to allow automatic firmware upgrades. |
| **dap** *dap-num* | Number of a Distributed AP on which to allow automatic firmware upgrades. |
| **dap auto** | Configures firmware upgrades for the AP configuration profile. |
| **enable** | Enables automatic firmware upgrades. |
| **disable** | Disables automatic firmware upgrades. |

**Defaults:** Automatic firmware upgrades of DWL-8220AP access points are enabled by default.

**Access:** Enabled.

**Usage:** When the feature is enabled on a DWS-1008 port, a DWL-8220AP access point connected to that port upgrades its boot firmware to the latest version stored on the switch while booting.

**Examples** The following command disables automatic firmware upgrades on the DWL-8220AP access point connected to port 2:

```
DWS-1008# set ap 2 upgrade-firmware disable
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set radio-profile active-scan

Disables or reenables active RF detection scanning on the DWL-8220AP radios managed by a radio profile. When active scanning is enabled, DWL-8220AP radios look for rogue devices by sending probe any requests (probe requests with a null SSID name), to solicit probe responses from other access points.

Passive scanning is always enabled and cannot be disabled. During passive scanning, radios look for rogues by listening for beacons and probe responses.

**Syntax: set radio-profile** *name* **active-scan {enable | disable}**

*name* Radio profile name.

**enable** Configures radios to actively scan for rogues.

**disable** Configures radios to scan only passively for rogues by listening for beacons and probe responses.

**Defaults:** Active scanning is enabled by default.

**Access:** Enabled.

**Usage:** You can enter this command on any DWS-1008 switch. The command takes effect only on that switch.

**Examples:** The following command disables active scan in radio profile *radprof3*:

```
DWS-1008# set radio-profile radprof3 active-scan disable
success: change accepted.
```

**See Also:**
• show radio-profile

# set radio-profile auto-tune channel-config

Disables or reenables dynamic channel tuning (RF Auto-Tuning) for the DWL-8220AP radios in a radio profile.

**Syntax: set radio-profile** *name* **auto-tune channel-config {enable | disable}**


Download from Www.Somanuals.com. All Manuals Search And Download.

*name* Radio profile name.

**enable** Configures radios to dynamically select their channels when the radios are started.

**disable** Configures radios to use their statically assigned channels, or the default channels if unassigned, when the radios are started.

**no-client** Configures radios to change channels regardless of client status. Without this option, a radio changes the channel only if the radio does not have any active clients on that channel.

**Defaults:** Dynamic channel assignment is enabled by default.

**Access:** Enabled.

**Usage:** If you disable RF Auto-Tuning for channels, MSS does not dynamically set the channels when radios are first enabled and also does not tune the channels during operation.

If RF Auto-Tuning for channels is enabled, MSS does not allow you to manually change channels.

**Examples:** The following command disables dynamic channel tuning for radios in the *rp2* radio profile:

```
DWS-1008# set radio-profile rp2 auto-tune channel-config disable
success: change accepted.
```

**See Also:**
- set {ap | dap} radio channel
- set radio-profile auto-tune channel-holddown
- set radio-profile auto-tune channel-interval
- set radio-profile auto-tune power-config
- show radio-profile

# set radio-profile auto-tune channel-holddown

Sets the minimum number of seconds a radio in a radio profile must remain at its current channel assignment before RF Auto-Tuning can change the channel. The channel holddown provides additional stability to the network by preventing the radio from changing channels too rapidly in response to spurious RF anomalies such as short-duration channel interference.

**Syntax: set radio-profile** *name* **auto-tune channel-holddown** *holddown rate*


Download from Www.Somanuals.com. All Manuals Search And Download.

*name* Radio profile name.

*rate* Minimum number of seconds a radio must remain on its current channel setting before RF Auto-Tuning is allowed to change the channel. You can specify from 0 to 65535 seconds.

**Defaults:** The default RF Auto-Tuning channel holddown is 900 seconds.

**Access:** Enabled.

**Usage:** The channel holddown applies even if RF anomalies occur that normally cause an immediate channel change.

**Examples:** The following command changes the channel holddown for radios in radio profile rp2 to 600 seconds:

```
DWS-1008# set radio-profile rp2 auto-tune channel-holddown 600
success: change accepted.
```

**See Also:**
- set radio-profile auto-tune channel-config
- set radio-profile auto-tune channel-interval
- set radio-profile auto-tune channel-lockdown
- show radio-profile

## set radio-profile auto-tune channel-interval

Sets the interval at which RF Auto-Tuning decides whether to change the channels on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio channels if needed.

**Syntax: set radio-profile** *name* **auto-tune channel-interval** *seconds*

*name* Radio profile name.

*seconds* Number of seconds RF Auto-Tuning waits before changing radio channels to adjust to RF changes, if needed. You can specify from 0 to 65535 seconds.

**Defaults:** The default channel interval is 3600 seconds (one hour).

**Access:** Enabled.

**Usage:** D-Link recommends that you use an interval of at least 300 seconds (5 minutes). RF Auto-Tuning can change a radio's channel before the channel interval expires in response to RF anomalies. Even in this case, channel changes cannot occur more frequently than the channel holddown interval.


Download from Www.Somanuals.com. All Manuals Search And Download.

If you set the interval to 0, RF Auto-Tuning does not reevaluate the channel at regular intervals. However, RF Auto-Tuning can still change the channel in response to RF anomalies.

**Examples:** The following command sets the channel interval for radios in radio profile *rp2* to 2700 seconds (45 minutes):

```
DWS-1008# set radio-profile rp2 auto-tune channel-interval 2700
success: change accepted.
```

## set radio-profile auto-tune channel-lockdown

Locks down the current channel settings on all radios in a radio profile. The channel settings that are in effect when the command is entered are changed into statically configured channel assignments on the radios. RF Auto-Tuning of channels is then disabled in the radio profile.

**Syntax: set radio-profile name auto-tune channel-lockdown**

*name* Radio profile name.

**Defaults:** By default, when RF Auto-Tuning of channels is enabled, channels continue to be changed dynamically based on network conditions.

**Access:** Enabled.

**Usage:** To save this command and the static channel configuration commands created when you enter this command, save the configuration.

**Examples:** The following command locks down the channel settings for radios in radio profile *rp2*:

```
DWS-1008# set radio-profile rp2 auto-tune channel-lockdown
success: change accepted.
```

**See Also:**
- set radio-profile auto-tune channel-config
- set radio-profile auto-tune channel-holddown
- set radio-profile auto-tune channel-interval
- show radio-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set radio-profile auto-tune power-config

Enables or disables dynamic power tuning (RF Auto-Tuning) for the DWL-8220AP radios in a radio profile.

**Syntax: set radio-profile** *name* **auto-tune power-config {enable | disable}**

| | |
|---|---|
| *name* | Radio profile name. |
| **enable** | Configures radios to dynamically set their power levels when the DWL- 8220APs are started. |
| **disable** | Configures radios to use their statically assigned power levels, or the default power levels if unassigned, when the radios are started. |

**Defaults:** Dynamic power assignment is disabled by default.

**Access:** Enabled.

**Usage:** When RF Auto-Tuning for power is disabled, MSS does not dynamically set the power levels when radios are first enabled and also does not tune power during operation with associated clients.

When RF Auto-Tuning for power is enabled, MSS does not allow you to manually change the power level.

**Examples:** The following command enables dynamic power tuning for radios in the *rp2* radio profile:

```
DWS-1008# set radio-profile rp2 auto-tune power-config enable
success: change accepted.
```

**See Also:**
- set {ap | dap} radio auto-tune max-power
- set radio-profile auto-tune channel-config
- set radio-profile auto-tune power-interval
- set radio-profile auto-tune power-lockdown
- set radio-profile auto-tune power-ramp-interval
- show radio-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set radio-profile auto-tune power-interval

Sets the interval at which RF Auto-Tuning decides whether to change the power level on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio power levels if needed.

**Syntax: set radio-profile** *name* **auto-tune power-interval** *seconds*

| | |
|---|---|
| *name* | Radio profile name. |
| *seconds* | Number of seconds MSS waits before changing radio power levels to adjust to RF changes, if needed. You can specify from 1 to 65535 seconds. |

**Defaults:** The default power tuning interval is 300 seconds.

**Access:** Enabled.

**Usage:** RF Auto-Tuning also can temporarily increase a radio's power level to preserve the minimum data rate for an associated client. In this case, the radio reduces its power in 1 dBm increments until the power returns to the expected level.

**Examples:** The following command sets the power interval for radios in radio profile *rp2* to 240 seconds:

```
DWS-1008# set radio-profile rp2 auto-tune power-interval 240
success: change accepted.
```

**See Also:**
- set {ap | dap} radio auto-tune max-power
- set radio-profile auto-tune channel-config
- set radio-profile auto-tune power-lockdown
- set radio-profile auto-tune power-ramp-interval
- show service profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set radio-profile auto-tune power-lockdown

Locks down the current power settings on all radios in a radio profile. The power settings that are in effect when the command is entered are changed into statically configured power settings on the radios. RF Auto-Tuning of power is then disabled in the radio profile.

**Syntax: set radio-profile** *name* **auto-tune power-lockdown**

*name* Radio profile name.

**Defaults:** By default, when RF Auto-Tuning of power is enabled, power settings continue to be changed dynamically based on network conditions.

**Access:** Enabled.

**Usage:** To save this command and the static power configuration commands created when you enter this command, save the configuration.

**Examples:** The following command locks down the power settings for radios in radio profile *rp2*:

```
DWS-1008# set radio-profile rp2 auto-tune power-lockdown
success: change accepted.
```

**See Also:**
- set {ap | dap} radio auto-tune max-power
- set radio-profile auto-tune channel-lockdown
- set radio-profile auto-tune power-config
- set radio-profile auto-tune power-interval
- set radio-profile auto-tune power-ramp-interval

# set radio-profile auto-tune power-ramp-interval

Changes the interval at which power is increased or decreased, in 1 dBm increments, on radios in a radio profile until the optimum power level calculated by RF Auto-Tuning is reached.

**Syntax: set radio-profile** *name* **auto-tune power-ramp-interval** *seconds*

*name* Radio profile name.

*seconds* Number of seconds MSS waits before increasing or decreasing radio power by another 1 dBm. You can specify from 1 to 65535.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** The default interval is 60 seconds.

**Access:** Enabled.

**Examples:** The following command changes the power ramp interval for radios in radio profile rp2 to 120 seconds:

```
DWS-1008# set radio-profile rp2 auto-tune power-ramp-interval 120
success: change accepted.
```

**See Also:**
- set {ap | dap} radio auto-tune max-power
- set radio-profile auto-tune power-config
- set radio-profile auto-tune power-interval
- set radio-profile auto-tune power-lockdown
- show radio-profile

# set radio-profile beacon-interval

Changes the rate at which each DWL-8220AP radio in a radio profile advertises its service set identifier (SSID).

**Syntax: set radio-profile** *name* **beacon-interval** *interval*

| | |
|---|---|
| *name* | Radio profile name. |
| *interval* | Number of milliseconds (ms) between beacons. You can specify from 25 ms to 8191 ms. |

**Defaults:** The beacon interval for DWL-8220AP radios is 100 ms by default.

**Access:** Enabled.

**Usage:** You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the set radio-profile mode command.

**Examples:** The following command changes the beacon interval for radio profile *rp1* to 200 ms:

```
DWS-1008# set radio-profile rp1 beacon-interval 200
success: change accepted.
```

**See Also:**
- set radio-profile mode
- show radio-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set radio-profile countermeasures

Countermeasures affect wireless service on a radio. When an AP radio is sending countermeasures, the radio is disabled for use by network traffic, until the radio finishes sending the countermeasures.

Enables or disables countermeasures for on the DWL-8220AP radios managed by a radio profile. Countermeasures are packets sent by a radio to prevent clients from being able to use rogue access points.

DWL-8220AP radios can also issue countermeasures against interfering devices. An interfering device is not part of the D-Link network but also is not a rogue. No client connected to the device has been detected communicating with any network entity listed in the forwarding database (FDD) of any DWS-1008 switch in the MobileLAN. Although the interfering device is not connected to your network, the device might be causing RF interference with
DWL-8220AP radios.

**Syntax: set radio-profile name countermeasures {all | rogue | configured | none}**

| | |
|---|---|
| *name* | Radio profile name. |
| **all** | Configures radios to attack rogues and interfering devices. |
| **rogue** | Configures radios to attack rogues only. |
| **configured** | Configures radios to attack only devices in the attack list on the DWS-1008 (on-demand countermeasures). When this option is specified, devices found to be rogues by other means, such as policy violations or by determining that the device is providing connectivity to the wired network, are not attacked. |
| **none** | Disables countermeasures for this radio profile. |

**Defaults:** Countermeasures are disabled by default.

**Access:** Enabled.

**Examples:** The following command enables countermeasures in radio profile *radprof3* for rogues only:

```
DWS-1008# set radio-profile radprof3 countermeasures rogue
success: change accepted.
```

The following command disables countermeasures in radio profile *radprof3*:

```
DWS-1008# clear radio-profile radprof3 countermeasures
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The following command causes radios managed by radio profile *radprof3* to issue countermeasures against devices in the DWS-1008's attack list:

```
DWS-1008# radio-profile radprof3 countermeasures configured
success: change accepted.
```

Note that when you issue this command, countermeasures are then issued only against devices in the DWS-1008's attack list, not against other devices that were classified as rogues by other means.

**See Also:**
- show radio-profile

# set radio-profile dtim-interval

Changes the number of times after every beacon that each DWL-8220AP radio in a radio profile sends a delivery traffic indication map (DTIM). An DWL-8220AP access point sends the multicast and broadcast frames stored in its buffers to clients who request them in response to the DTIM.

**Note:** The DTIM interval applies to both the beaconed SSID and the nonbeaconed SSID.

**Syntax: set radio-profile** *name* **beacon-interval** *interval*

| | |
|---|---|
| *name* | Radio profile name. |
| *interval* | Number of times the DTIM is transmitted after every beacon. You can enter a value from 1 through 31. |

**Defaults:** By default, DWL-8220AP access points send the DTIM once after each beacon.

**Access:** Enabled.

**Usage:** You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

The DTIM interval does not apply to unicast frames.

**Examples:** The following command changes the DTIM interval for radio profile rp1 to 2:

```
DWS-1008# set radio-profile rp1 dtim-interval 2
success: change accepted.
```

**See Also:**
- set radio-profile mode
- show radio-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set radio-profile frag-threshold

Changes the fragmentation threshold for the DWL-8220AP radios in a radio profile. The fragmentation threshold is the threshold at which the long-retry-count is applicable instead of the short-retry-count.

The long-retry-count specifies the number of times a radio can send a unicast frame that is equal to or longer than the frag-threshold without receiving an acknowledgment.

The short-retry-count specifies the number of times a radio can send a unicast frame that is shorter than the frag-threshold without receiving an acknowledgment.

**Syntax: set radio-profile** *name* **frag-threshold** *threshold*

| | |
|---|---|
| *name* | Radio profile name. |
| *threshold* | Maximum frame length, in bytes. You can enter a value from 256 through 2346. |

**Defaults:** The default fragmentation threshold for DWL-8220AP radios is 2346 bytes.

**Access:** Enabled.

**Usage:** You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

The frag-threshold does not specify the maximum length a frame is allowed to be without being broken into multiple frames before transmission.

The frag-threshold does not change the RTS threshold, which specifies the maximum length a frame can be before the radio uses the RTS/CTS method to send the frame. To change the RTS threshold, use the **set radio-profile rts-threshold** command instead.

**Examples:** The following command changes the fragmentation threshold for radio profile *rp1* to 1500 bytes:

```
DWS-1008# set radio-profile rp1 frag-threshold 1500
success: change accepted.
```

**See Also:**
- set radio-profile mode
- set radio-profile rts-threshold
- set service-profile long-retry-count
- set service-profile short-retry-count
- show radio-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set radio-profile max-rx-lifetime

Changes the maximum receive threshold for the DWL-8220AP radios in a radio profile. The maximum receive threshold specifies the number of milliseconds that a frame received by a radio can remain in buffer memory.

**Syntax: set radio-profile** *name* **max-rx-lifetime** *time*

*name* Radio profile name.

*time* Number of milliseconds. You can enter a value from 500 (0.5 second) through 250,000 (250 seconds).

**Defaults:** The default maximum receive threshold for DWL-8220AP radios is 2000ms (2 seconds).

**Access:** Enabled.

**Usage:** You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

**Examples:** The following command changes the maximum receive threshold for radio profile *rp1* to 4000 ms:

```
DWS-1008# set radio-profile rp1 max-rx-lifetime 4000
success: change accepted.
```

**See Also:**
- set radio-profile mode
- set radio-profile max-tx-lifetime
- show radio-profile

# set radio-profile max-tx-lifetime

Changes the maximum transmit threshold for the DWL-8220AP radios in a radio profile. The maximum transmit threshold specifies the number of milliseconds that a frame scheduled to be transmitted by a radio can remain in buffer memory.

**Syntax: set radio-profile** *name* **max-tx-lifetime** *time*

*name* Radio profile name.

*time* Number of milliseconds. You can enter a value from 500 (0.5 second) through 250,000 (250 seconds).


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** The default maximum receive threshold for DWL-8220AP radios is 2000ms (2 seconds).

**Access:** Enabled.

**Usage:** You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

**Examples:** The following command changes the maximum transmit threshold for radio profile rp1 to 4000 ms:

```
DWS-1008# set radio-profile rp1 max-tx-lifetime 4000
success: change accepted.
```

**See Also:**
- set radio-profile mode
- set radio-profile max-tx-lifetime
- show radio-profile

# set radio-profile mode

Creates a new radio profile, or disables or reenables all DWL-8220AP radios that are using a specific profile.

**Syntax: set radio-profile** *name* **[mode {enable | disable}]**

| | |
|---|---|
| **radio-profile** *name* | Radio profile name of up to 16 alphanumeric characters, with no spaces.<br><br>Use this command without the mode enable or mode disable option to create a new profile. |
| **mode enable** | Enables the radios that use this profile. |
| **mode disable** | Disables the radios that use this profile. |

**Defaults:** Each radio profile that you create has a set of properties with factory default values that you can change with the other set radio-profile commands in this chapter.


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below lists the parameters controlled by a radio profile and their default values.

| Parameter | Default Value | Radio Behavior When Parameter Set to Default Value |
|---|---|---|
| active-scan | enable | Sends probe any requests (probe requests with a null SSID name) to solicit probe responses from other access points. |
| auto-tune | enable | Allows dynamic configuration of channel and power settings by MMS. |
| beacon-interval | 100 | Waits 100ms between beacons. |
| countermeasures | Not configured | Does not issue countermeasures against any device. |
| dtim-interval | 1 | Sends the delivery traffic indication map (DTIM) after every beacon. |
| frag-threshold | 2346 | Uses the short-retry-count for frames shorter than 2346 bytes and uses the long-retry-count for frames that are 2346 bytes or longer. |
| max-rx-lifetime | 2000 | Allows a received frame to stay in the buffer for up to 2000ms (2 seconds). |
| max-tx-lifetime | 2000 | Allows a frame that is scheduled for transmission to stay in the buffer for up to 2000ms (2 seconds). |
| preamble-length | short | Advertises support for short 802.11b preambles, and generates unicast frames with the preamble length specified by the client.<br><br>Note: This parameter applies only to 802.11b/g radios. |
| qos-mode | wmm | Classifies and marks traffic based on 802.1q and DSCP, and optimizes forwarding prioritization of AP radios for Wi-Fi Multimedia (WMM). |
| rfid-mode | disable | Radio does not funtion as a location reciever in an AreoScout Visibility System. |
| rts-threshold | 2346 | Transmits frames longer than 2346 bytes by means of the Request-to-Send/Clear-to-Send (RTS/CTS) method. |
| service-profile | No service profiles defined | You must configure a service profile. The service profile sets the SSID name and other parameters. |
| wmm-powersave | disable | Requires clients to send a seperate PSpoll to retrieve each unicast packet buffered by the AP. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Access:** Enabled.

**Usage:** Use the command without any optional parameters to create new profile. If the radio profile does not already exist, MSS creates a new radio profile. Use the enable or disable option to enable or disable all the radios using a profile. To assign the profile to one or more radios, use the **set ap radio radio-profile** command.

To change a parameter in a radio profile, you must first disable all the radios in the profile. After you complete the change, you can reenable the radios.

To enable or disable specific radios without disabling all of them, use the **set ap radio** command.

**Examples:** The following command configures a new radio profile named *rp1*:

```
DWS-1008# set radio-profile rp1
success: change accepted.
```

The following command enables the radios that use radio profile *rp1*:

```
DWS-1008# set radio-profile rp1 mode enable
success: change accepted.
```

The following commands disable the radios that use radio profile *rp1*, change the beacon interval, then reenable the radios:

```
DWS-1008# set radio-profile rp1 mode disable
DWS-1008# set radio-profile rp1 beacon-interval 200
DWS-1008# set radio-profile rp1 mode enable
```

The following command enables the WPA IE on AP radios in radio profile *rp2*:

```
DWS-1008# set radio-profile rp1 mode enable
success: change accepted.
```

**See Also:**

- set radio-profile mode
- set {ap | dap} radio radio-profile
- show {ap | dap} config
- show radio-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set radio-profile preamble-length

Changes the preamble length for which an 802.11b/g DWL-8220AP radio advertises support. This command does not apply to 802.11a.

**Syntax: set radio-profile** *name* **preamble-length {long | short}**

| | |
|---|---|
| *name* | Radio profile name. |
| **long** | Advertises support for long preambles. |
| **short** | Advertises support for short preambles. |

**Defaults:** The default is **short**.

**Access:** Enabled.

**Usage:** Changing the preamble length value affects only the support advertised by the radio. Regardless of the preamble length setting (short or long), an 802.11b/g radio accepts and can generate 802.11b/g frames with either short or long preambles.

If a client associated with an 802.11b/g radio uses long preambles for unicast traffic, the DWL-8220AP access point still accepts frames with short preambles but does not transmit frames with short preambles. This change also occurs if the access point overhears a beacon from an 802.11b/g radio on another access point that indicates the radio has clients that require long preambles.

You must disable all radios that use a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

**Examples:** The following command configures 802.11b/g radios that use the radio profile *rp_long* to advertise support for long preambles instead of short preambles:

```
DWS-1008# set radio-profile rp_long preamble-length long
success: change accepted.
```

**See Also:**
- set radio-profile mode
- show radio-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set radio-profile qos-mode

Sets the prioritization mode for forwarding queues on AP radios managed by the radio profile.

**Syntax: set radio-profile** *name* **qos-mode {svp | wmm}**

*name* Radio profile name.

**svp** Optimizes forwarding prioritization of AP radios for SpectraLink Voice Priority (SVP).

**wmm** Classifies and marks traffic based on 802.1p and DSCP, and optimizes forwarding prioritization of AP radios for Wi-Fi Multimedia (WMM).

**Defaults:** The default QoS mode is **wmm**.

**Access:** Enabled.

**Usage:** When SVP is enabled, AP forwarding prioritization is optimized for SpectraLink Voice Priority (SVP) instead of WMM, and the AP does not tag packets it sends to the DWS-1008. Otherwise, classification and tagging remain in effect.

If you plan to use SVP or another non-WMM type of prioritization, you must configure ACLs to tag the packets.

**Examples:** The following command changes the QoS mode for radio profile *rp1* to SVP:

```
DWS-1008# set radio-profile rp1 qos-mode svp
success: change accepted.
```

**See Also:**
- set radio-profile mode 6
- show radio-profile

# set radio-profile rfid-mode

Enables AP radios managed by a radio profile to function as location receivers in an AeroScout Visibility System. An AeroScout Visibility System allows system administrators to track mobile assets using RFID tags.

When you enable RFID mode on a radio profile, radios in the profile can receive and process signals transmitted by RFID tags and relay them with related information to the AeroScout Engine.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Syntax: set radio-profile** *name* **rfid-mode {enable | disable}**

*name* Radio profile name.

**enable** Enables radios to function as asset location receivers.

**disable** Disables radios from functioning as asset location receivers.

**Defaults:** The default is **disable**.

**Access:** Enabled.

**Examples:** The following command enables radios managed by radio profile *rp1* to act as asset location receivers:

```
DWS-1008# set radio-profile rfid-mode enable
success: change accepted.
```

**See Also:**
- set radio-profile mode
- show radio-profile

# set radio-profile rts-threshold

Changes the RTS threshold for the AP radios in a radio profile. The RTS threshold specifies the maximum length a frame can be before the radio uses the RTS/CTS method to send the frame. The RTS/CTS method clears the air of other traffic to avoid corruption of the frame due to a collision with another frame.

**Syntax: set radio-profile** *name* **rts-threshold** *threshold*

*name* Radio profile name.

*threshold* Maximum frame length, in bytes. You can enter a value from 256 through 3000.

**Defaults:** The default RTS threshold is 2346 bytes.

**Access:** Enabled.

**Usage:** You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command changes the RTS threshold for radio profile *rp1* to 1500 bytes:

```
DWS-1008# set radio-profile rp1 rts-threshold 1500
success: change accepted.
```

**See Also:**
- set radio-profile mode
- show radio-profile

# set radio-profile service-profile

Maps a service profile to a radio profile. All radios that use the radio profile also use the parameter settings, including SSID and encryption settings, in the service profile.

**Syntax: set radio-profile** *name* **service-profile** *name*

| | |
|---|---|
| **radio-profile** *name* | Radio profile name of up to 16 alphanumeric characters, with no spaces. |
| **service-profile** *name* | Service profile name of up to 16 alphanumeric characters, with no spaces. |

**Defaults:** A radio profile does not have a service profile associated with it by default. In this case, the radios in the radio profile use the default settings for parameters controlled by the service profile. The following table lists the parameters controlled by a service profile and their default values.

| Parameter | Default Value | Radio Behavior When Parameter Set to Default Value |
|---|---|---|
| attr | No attributes configured | Does not assign the SSID's authorization attribute values to SSID users, even if attributes are not otherwise assigned. |
| auth-dot1x | enable | When the Wi-Fi Protected Access (WPA) information element (IE) is enabled, uses 802.1X to authenticate WPA clients. |
| auth-fallthru | none | Denies access to users who do not match an 802.1X or MAC authentication fule for the SSID requested by the user. |
| auth-psk | none | Does not support using a preshared key (PSK) to authenticate WPA clients. |
| beacon | enable | Sends beacons to advertise the SSID managed by the service profile. |


Download from Www.Somanuals.com. All Manuals Search And Download.

## Table: Defaults for Radio Profile Parameters (continued)

| Parameter | Default Value | Radio Behavior When Parameter Set to Default Value |
|---|---|---|
| cac-mode | none | Does not limit the number of active user sessions based on Call Admission Control. |
| cac-session | 14 | If session-based CAC is enabled (**cac-mode** is set to **session**), limits the number of active user sessions on a radio to 14. |
| cipher-ccmp | disable | Does not use Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) to encrypt traffic sent to WPA clients. |
| cipher-tkip | enable | When WPA IE is enabled, uses Temporal Key Integrity Protocol (TKIP) to encryp traffic sent to WPA clients. |
| cipher-wep104 | disable | Does not use Wired Equivalent Privacy with 104-bit keys to encrypt traffic sent to WPA clients. |
| cipher-wep40 | disable | Does not user WEP with 40-bit keys to encrypt traffic sent to WPA clents. |
| cos | 0 | If static CoS is enabled (**static-cos** is set to **enable**) assigns CoS to all data traffic to or from clients. |
| dhcp-restrict | disable | Does not restrict a client's traffic to only DHCP traffic while the client is being authenticated and authorized. |
| idle-client-probing | enable | Sends a keepalive packet (a null-data frame) to each client every 10 seconds. |
| keep-initial-vlan | disable | Reassigns the user to a VLAN after roaming, instead of leaving the roamed user on the VLAN assigned by the switch where the user is logged on.<br><br>**Note:** Enabling the option does not retain the user's initial VLAN assignment in all cases. |
| long-retry-count | 5 | Sends a long unicast frame up to five times without acknowledgement. |
| no-broadcast | disable | Does not reduce wireless broadcast traffic by sending unicasts to clients for ARP requests and DHCP Offers and Acks instead of forwarding them as multicasts. |
| proxy-arp | disable | Does not reply on behalf of wireless clients to ARP requests for client IP addresses. Instead, the radio forwards the ARP Requests as wireless broadcasts. |


Download from Www.Somanuals.com. All Manuals Search And Download.

## Table: Defaults for Radio Profile Parameters (continued)

| Parameter | Default Value | Radio Behavior When Parameter Set to Default Value |
|---|---|---|
| psk-phrase | No passphrase defined | Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients. |
| psk-raw | No preshared key defined | Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients. |
| rsn-ie | disable | Does not use the RSN IE in transmitted frames. (The RSN IE is required for 802.11i. RSN is sometimes called *WPA2*.) |
| shared-key-auth | disable | Does not use shared-key authentication.<br><br>This parameter does not enable PSK authentication for WPA. To enable PSK encryption for WPA, use the **set radio-profile auth-psk** command. |
| short-retry-count | 5 | Sends a short unicast frame up to five times without acknowledgment. |
| soda | disable | Sygate On Demand Agent (SODA) files are not downloaded to connecting clients. |
| ssid-name | dlink | Uses the SSID name *dlink*. |
| static-cos | disable | Assigns CoS based on the Qos mode (**wmm** or **svp**) or based on ALCs. |
| tkip-me-time | 6000 | Uses Michael countermeasures for 60,000ms (60 seconds) followin detertion of a second MIC failure within 60 seconds. |
| transmit-rates | 802.11a:<br>• mandantory: 6.0, 12.0, 24.0<br>• beacon rate: 6.0<br>• multicast-rate: auto<br>• disabled: none<br><br>802.11b:<br>• mandantory: 1.0, 2.0<br>• beacon rate: 2.0<br>• multicast-rate: auto<br>• disabled: none<br><br>802.11g:<br>• mandantory: 1.0, 2.0, 5.5, 11.0<br>• beacon rate: 2.0<br>• multicast-rate: auto<br>• disabled: none | Accepts associations only from clients that support one of the mandantory rates.<br><br>Sends beacons at the specified rate (6Mbps for 802.11a, 2Mbps for 802.11b/g.<br><br>Sends multicast data at the highest rate that can reach all clients connected to the radio.<br><br>Accepts frames from clients at all valid data rates. (No rates are disabled by default.) |


Download from Www.Somanuals.com. All Manuals Search And Download.

## Table: Defaults for Radio Profile Parameters (continued)

| Parameter | Default Value | Radio Behavior When Parameter Set to Default Value |
|---|---|---|
| user-idle-timeout | 180 | Allows a client to remain idle for 180 seconds (3 minutes) before MSS changes the client's session to the Disassociated state. |
| web-portal-acl | portalacl<br><br>Note: This is the default only if the fallthru type on the service profile has been set to web-portal. Otherwise, the value is unconfigured. | If set to **portalacl** and the service profile fallthru is set to **web-portal**, radios use the *portalacl* ACL to filter traffic for Web Portal users during authentication.<br><br>If the fallthru type is not **web-portal**, radios do not use the **web-portal-acl** setting. |
| web-portal-form | Not configured | For WebAAA users, serves the D-Link login page. |
| web-portal-session-timeout | 5 | Allows a Web Portal WebAAA session to remain in the Deassociated state 5 seconds before being terminated automatically. |
| wep key-index | No Keys defined | Uses dynamic WEP rather than static WEP.<br><br>**Note:** If you configure a WEP key for static WEP, MSS continues to also support dynamic WEP. |
| web active-multicast-index | 1 | Uses WEP key 1 for static WEP encryption of multicast traffic if WEP encryption is enabled and keys are defined. |
| wep active-unicast -index | 1 | Uses WEP key 1 for static WEP encryption of unicast traffic if WEP encryption is enabled and keys are defined. |
| wpa-ie | disable | Does not use the WPA IE in transmitted frames. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Access:** Enabled.

**Usage:** You must configure the service profile before you can map it to a radio profile. You can map the same service profile to more than one radio profile.

You must disable all radios that use a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

**Examples:** The following command maps service-profile wpa_clients to radio profile *rp2*:

```
DWS-1008# set radio-profile rp2 service-profile wpa_clients
success: change accepted.
```

# set radio-profile wmm-powersave

Enables Unscheduled Automatic Powersave Delivery (U-APSD) on AP radios managed by the radio profile. U-APSD enables WMM clients that use powersave mode to more efficiently request buffered unicast packets from AP radios.

When U-APSD is enabled, a client can retrieve buffered unicast packets for a traffic priority enabled for U-APSD by sending a QoS data or QoS-Null frame for that priority. U-APSD can be enabled for individual traffic priorities, for individual clients, based on the client's request. A client enables U-APSD for a traffic priority by indicating this preference when (re)associating with the AP radio.

A client can but is not required to request U-APSD for all four traffic priorities.


Download from Www.Somanuals.com. All Manuals Search And Download.

The AP radio still buffers packets for all traffic priorities even if the client does not request U-APSD for them. However, to retrieve buffered packets for priorities that are not using U-APSD, a client must send a separate PSpoll for each buffered packet.

**Syntax: set radio-profile name wmm-powersave {enable | disable}**

*name* Radio profile name.

**enable** Enables U-APSD.

**disable** Disables U-APSD.

**Defaults:** U-APSD is disabled by default.

**Access:** Enabled.

**Usage:** U-APSD is supported only for QoS mode WMM. If WMM is not enabled on the radio profile, use the set radio-profile qos-mode command to enable it.

**Examples:** The following command enables U-APSD on radio profile *rp1*:

```
DWS-1008# set radio-profile rp1 wmm-powersave enable
success: change accepted.
```

**See Also:**
- set radio-profile mode
- set radio-profile qos-mode
- show radio-profile

# set service-profile attr

Configures authorization attributes that are applied by default to users accessing the SSID managed by the service profile. These SSID default attributes are applied in addition to any supplied by the RADIUS server or from the local database.

**Syntax: set service-profile** *name* **attr** *attribute-name value*

*name* Service profile name.

*attribute-name value* Name and value of an attribute you are using to authorize SSID users for a particular service or session characteristic.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** By default, a service profile does not have any authorization attributes set.

**Access:** Enabled.

**Usage:** To change the value of a default attribute for a service profile, use the **set service-profile attr** command and specify a new value.

The SSID default attributes are applied in addition to any attributes supplied for the user by the RADIUS server or the local database. When the same attribute is specified both as an SSID default attribute and through AAA, then the attribute supplied by the RADIUS server or the local database takes precedence over the SSID default attribute. If a location policy is configured, the location policy rules also take precedence over SSID default attributes. The SSID default attributes serve as a fallback when neither the AAA process, nor a location policy, provides them.

For example, a service profile might be configured with the **service-type** attribute set to *2*. If a user accessing the SSID is authenticated by a RADIUS server, and the RADIUS server returns the **vlan-name** attribute set to *orange*, then that user will have a total of two attributes set: **service-type** and **vlan-name**.

If the service profile is configured with the **vlan-name** attribute set to *blue*, and the RADIUS server returns the **vlan-name** attribute set to *orange*, then the attribute from the RADIUS server takes precedence; the user is placed in the orange VLAN.

You can display the attributes for each connected user and whether they are set through AAA or through SSID defaults by entering the **show sessions network verbose** command. You can display the configured SSID defaults by entering the **show service-profile** command.

**Examples:** The following command assigns users accessing the SSID managed by service profile *sp2* to VLAN *blue*:

```
DWS-1008# set service-prof sp2 attr vlan-name blue
success: change accepted.
```

The following command limits the days and times when users accessing the SSID managed by service profile *sp2* can access the network, to 5 p.m. to 2 a.m. every weekday, and all day Saturday and Sunday:

```
DWS-1008# set service-prof sp2 attr time-of-day Wk1700-0200,Sa,Su
success: change accepted.
```

**See Also:**
- show service-profile
- show sessions network


Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile auth-dot1x

Disables or reenables 802.1X authentication of Wi-Fi Protected Access (WPA) clients by AP radios, when the WPA information element (IE) is enabled in the service profile that is mapped to the radio profile that the radios are using.

**Syntax: set service-profile name auth-dot1x {enable | disable}**

*name* Service profile name.

**enable** Enables 802.1X authentication of WPA clients.

**disable** Disables 802.1X authentication of WPA clients.

**Defaults:** When the WPA IE is enabled, 802.1X authentication of WPA clients is enabled by default. If the WPA IE is disabled, the auth-dot1x setting has no effect.

**Access:** Enabled.

**Usage:** This command does not disable dynamic WEP for non-WPA clients. To disable dynamic WEP for non-WPA clients, enable the WPA IE (if not already enabled) and disable the 40-bit WEP and 104-bit WEP cipher suites in the WPA IE, if they are not already disabled.

To use 802.1X authentication for WPA clients, you also must enable the WPA IE.

If you disable 802.1X authentication of WPA clients, the only method available for authenticating the clients is preshared key (PSK) authentication. To use this, you must enable PSK support and configure a passphrase or key.

**Examples:** The following command disables 802.1X authentication for WPA clients that use service profile *wpa_clients*:

```
DWS-1008# set service-profile wpa_clients auth-dot1x disable
success: change accepted.
```

**See Also:**
- set service-profile auth-psk
- set service-profile psk-phrase
- set service-profile wpa-ie
- show service-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile auth-fallthru

Specifies the authentication type for users who do not match an 802.1X or MAC authentication rule for an SSID managed by the service profile. When a user tries to associate with an SSID, MSS checks the authentication rules for that SSID for a userglob that matches the username. If the SSID does not have an authentication rule that matches the username, authentication for the user *falls through* to the fallthru type.

The fallthru type is a service profile parameter, and applies to all radios within the radio profiles that are mapped to the service profile.

**Syntax: set service-profile** *name* **auth-fallthru {last-resort | none | web-portal}**

**last-resort** Automatically authenticates the user and allows access to the SSID requested by the user, without requiring a username and password.

**none** Denies authentication and prohibits the user from accessing the SSID.

**Note:** The fallthru authentication type **none** is different from the authentication method **none** you can specify for administrative access. The fallthru authentication type **none** denies access to a network user. In contrast, the authentication method **none** allows access to the DWS-1008 by an administrator.

**web-portal** Serves the user a web page from the DWS-1008's nonvolatile storage for secure login to the network.

**Defaults:** The default fallthru authentication type is none.

If a username does not match a userglob in an authentication rule for the SSID requested by the user, the DWS-1008 that is managing the radio the user is connected to redirects the user to a web page located on the DWS-1008. The user must type a valid username and password on the web page to access the SSID.

**Access:** Enabled.

**Usage** The **last-resort** fallthru authentication type allows any user to access any SSID managed by the service profile. This method does not require the user to provide a username or password. Use the **last-resort** method only if none of the SSIDs managed by the service profile require secure access.

The web-portal authentication type also requires additional configuration items.

**Examples:** The following command sets the fallthru authentication type for SSIDS managed by


Download from Www.Somanuals.com. All Manuals Search And Download.

the service profile rnd_lab to web-portal:

```
DWS-1008# set service-profile rnd_lab auth-fallthru web-portal
success: change accepted.
```

**See Also:**
- set web-portal
- set service-profile web-portal-form
- show service-profile

# set service-profile auth-psk

Enables preshared key (PSK) authentication of Wi-Fi Protected Access (WPA) clients by AP radios in a radio profile, when the WPA information element (IE) is enabled in the service profile.

**Syntax: set service-profile** *name* **auth-psk {enable | disable}**

| | |
|---|---|
| *name* | Service profile name. |
| **enable** | Enables PSK authentication of WPA clients. |
| **disable** | Disables PSK authentication of WPA clients. |

**Defaults:** When the WPA IE is enabled, PSK authentication of WPA clients is enabled by default. If the WPA IE is disabled, the **auth-psk** setting has no effect.

**Access:** Enabled.

**Usage:** This command affects authentication of WPA clients only.

To use PSK authentication, you also must configure a passphrase or key. In addition, you must enable the WPA IE.

**Examples:** The following command enables PSK authentication for service profile *wpa_clients*:

```
DWS-1008# set service-profile wpa_clients auth-psk enable
success: change accepted.
```

**See Also:**
- set service-profile auth-dot1x
- set service-profile psk-raw 7
- set service-profile wpa-ie
- show service-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile beacon

Disables or reenables beaconing of the SSID managed by the service profile.

An AP radio responds to an 802.11 probe any request with only the beaconed SSID(s). For a nonbeaconed SSID, radios respond only to directed 802.11 *probe* requests that match the nonbeaconed SSID's SSID string.

When you disable beaconing for an SSID, the radio still sends beacon frames, but the SSID name in the frames is blank.

**Syntax: set service-profile** *name* **beacon {enable | disable}**

*name* Service profile name.

**enable** Enables beaconing of the SSID managed by the service profile.

**disable** Disables beaconing of the SSID managed by the service profile.

**Defaults:** Beaconing is enabled by default.

**Access:** Enabled.

**Examples:** The following command disables beaconing of the SSID managed by service profile *sp2*:

```
DWS-1008# set service-profile sp2 beacon disable
success: change accepted.
```

**See Also:**
- set radio-profile beacon-interval
- set service-profile ssid-name
- set service-profile ssid-type
- show service-profile

# set service-profile cac-mode

Configures the Call Admission Control (CAC) mode.

**Syntax: set service-profile** *name* **cac-mode {none | session}**


Download from Www.Somanuals.com. All Manuals Search And Download.

*name* Service profile name.

**none** CAC is not used.

**session** CAC is based on the number of active sessions.

**Defaults:** The default CAC mode is **none**.

**Access:** Enabled.

**Examples:** The following command enables session-based CAC on service profile *sp1*:

```
DWS-1008# set service-profile sp1 cac-mode session
success: change accepted.
```

**See Also:**
- set service-profile cac-session
- show service-profile

# set service-profile cac-session

Specifies the maximum number of active sessions a radio can have when session-based CAC is enabled. When an DWL-8220AP has reached the maximum allowed number of active sessions, the radio refuses connections from additional clients.

**Syntax: set service-profile** *name* **cac-session** *max-sessions*

*name* Service profile name.

*max-sessions* Maximum number of active sessions allowed on the radio.

**Defaults:** The default number of sessions allowed is 14.

**Access:** Enabled.

**Usage:** This command applies only when the CAC mode is **session**. If the CAC mode is **none**, you can still change the maximum number of sessions, but the setting does not take effect until you change the CAC mode to **session**. To change the CAC mode, use the **set service-profile cac-mode** command.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command changes the maximum number of sessions for radios used by service profile *sp1* to 10:

```
DWS-1008# set service-profile sp1 cac-session 10
success: change accepted.
```

**See Also:**
- set service-profile cac-mode
- show service-profile

# set service-profile cipher-ccmp

Enables Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption with WPA clients, for a service profile.

**Syntax: set service-profile** *name* **cipher-ccmp {enable | disable}**

*name* Service profile name.

**enable** Enables CCMP encryption for WPA clients.

**disable** Disables CCMP encryption for WPA clients.

**Defaults:** CCMP encryption is disabled by default.

**Access:** Enabled.

**Usage:** To use CCMP, you must also enable the WPA IE.

**Examples:** The following command configures service profile *sp2* to use CCMP encryption:

```
DWS-1008# set service-profile sp2 cipher-ccmp enable
success: change accepted.
```

**See Also:**
- set service-profile cipher-tkip
- set service-profile cipher-wep104
- set service-profile cipher-wep40
- set service-profile wpa-ie
- show service-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile cipher-tkip

Disables or reenables Temporal Key Integrity Protocol (TKIP) encryption in a service profile.

**Syntax: set service-profile** *name* **cipher-ccmp {enable | disable}**

*name* Service profile name.

**enable** Enables TKIP encryption for WPA clients.

**disable** Disables TKIP encryption for WPA clients.

**Defaults:** When the WPA IE is enabled, TKIP encryption is enabled by default.

**Access:** Enabled.

**Usage:** To use TKIP, you must also enable the WPA IE.

**Examples:** The following command disables TKIP encryption in service profile *sp2*:

```
DWS-1008# set service-profile sp2 cipher-tkip disable
success: change accepted.
```

**See Also:**
- set service-profile cipher-ccmp
- set service-profile cipher-wep104
- set service-profile cipher-wep40
- set service-profile wpa-ie
- show service-profile

# set service-profile cipher-wep104

Enables dynamic Wired Equivalent Privacy (WEP) with 104-bit keys, in a service profile.

**Syntax: set service-profile** *name* **cipher-wep104 {enable | disable}**

*name* Service profile name.

**enable** Enables 104-bit WEP encryption for WPA clients.

**disable** Disables 104-bit WEP encryption for WPA clients.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** 104-bit WEP encryption is disabled by default.

**Access:** Enabled.

**Usage:** To use 104-bit WEP with WPA clients, you must also enable the WPA IE.

When 104-bit WEP in WPA is enabled in the service profile, radios managed by a radio profile that is mapped to the service profile can also support non-WPA clients that use dynamic WEP.

To support WPA clients that use 40-bit dynamic WEP, you must enable WEP with 40-bit keys. Use the **set service-profile cipher-wep40** command.

Microsoft Windows XP does not support WEP with WPA. To configure a service profile to provide dynamic WEP for XP clients, leave WPA disabled and use the **set service-profile wep** commands.

To support non-WPA clients that use static WEP, you must configure static WEP keys. Use the **set service-profile wep key-index** command.

**Examples:** The following command configures service profile *sp2* to use 104-bit WEP encryption:

```
DWS-1008# set service-profile sp2 cipher-wep104 enable
success: change accepted.
```

**See Also:**
- set service-profile cipher-ccmp
- set service-profile cipher-tkip
- set service-profile cipher-wep40
- set service-profile wep key-index
- set service-profile wpa-ie
- show service-profile

# set service-profile cipher-wep40

Enables dynamic Wired Equivalent Privacy (WEP) with 40-bit keys, in a service profile.

**Syntax: set service-profile** *name* **cipher-ccmp {enable | disable}**

| | |
|---|---|
| *name* | Service profile name. |
| **enable** | Enables 40-bit WEP encryption for WPA clients. |
| **disable** | Disables 40-bit WEP encryption for WPA clients. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** 40-bit WEP encryption is disabled by default.

**Access:** Enabled.

**Usage:** To use 40-bit WEP with WPA clients, you must also enable the WPA IE.

When 40-bit WEP in WPA is enabled in the service profile, radios managed by a radio profile that is mapped to the service profile can also support non-WPA clients that use dynamic WEP.

To support WPA clients that use 104-bit dynamic WEP, you must enable WEP with 104-bit keys in the service profile. Use the **set service-profile cipher-wep104** command.

Microsoft Windows XP does not support WEP with WPA. To configure a service profile to provide dynamic WEP for XP clients, leave WPA disabled and use the **set service-profile wep** commands.

To support non-WPA clients that use static WEP, you must configure static WEP keys. Use the **set service-profile wep key-index** command.

**Examples:** The following command configures service profile *sp2* to use 40-bit WEP encryption:

```
DWS-1008# set service-profile sp2 cipher-wep40 enable
success: change accepted.
```

**See Also:**
- set service-profile cipher-ccmp
- set service-profile cipher-tkip
- set service-profile cipher-wep40
- set service-profile wpa-ie
- show service-profile

# set service-profile cos

Sets the Class-of-Service (CoS) level for static CoS.

**Syntax: set service-profile** *name* **cos** *level*

*name* Service profile name.

*level* CoS value assigned by the AP to all traffic in the service profile.

**Defaults:** The default static CoS level is 0.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** This command applies only when static CoS is enabled. If static CoS is disabled, prioritization is based on the QoS mode configured in the radio profile, and on any ACLs that set CoS. To enable static CoS, use the **set service-profile static-cos** command.

**Examples:** The following command changes the static CoS level to 7 (voice priority):

```
DWS-1008# set service-profile sp1 cos 7
success: change accepted.
```

**See Also:**
- set service-profile static-cos
- show service-profile

# set service-profile dhcp-restrict

Enables or disables DHCP Restrict on a service profile. DHCP Restrict filters a newly associated client's traffic to allow DHCP traffic only, until the client has been authenticated and authorized. All other traffic is captured by the DWS-1008 and is not forwarded. After the client is successfully authorized, the traffic restriction is removed.

**Syntax: set service-profile** *name* **dhcp-restrict {enable | disable}**

| | |
|---|---|
| *name* | Service profile name. |
| **enable** | Enables DHCP Restrict. |
| **disable** | Disables DHCP Restrict. |

**Defaults:** DHCP Restrict is disabled by default.

**Access:** Enabled.

**Usage:** To further reduce the overhead of DHCP traffic, use the set service-profile no-broadcast command to disable DHCP broadcast traffic from AP radios to clients on the service profile's SSID.

**Examples:** The following command enables DHCP Restrict on service profile *sp1*:

```
DWS-1008# set service-profile sp1 dhcp-restrict enable
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile idle-client-probing

Disables or reenables periodic keepalives from AP radios to clients on a service profile's SSID. When idle-client probing is enabled, the AP radio sends a unicast null-data frame to each client every 10 seconds. Normally, a client that is still active sends an Ack in reply to the keepalive.

If a client does not send any data or respond to any keepalives before the user idle timeout expires, MSS changes the client's session to the Disassociated state.

**Syntax: set service-profile** *name* **idle-client-probing {enable | disable}**

*name* Service profile name.

**enable** Enables keepalives.

**disable** Disables keepalives.

**Defaults:** Idle-client probing is enabled by default.

**Access:** Enabled.

**Usage:** The length of time a client can remain idle (unresponsive to idle-client probes) is specified by the **user-idle-timeout** command.

**Examples:** The following command disables idle-client keepalives on service profile *sp1*:

```
DWS-1008# set service-profile sp1 idle-client-probing disable
success: change accepted.
```

**See Also:**
- set service-profile user-idle-timeout
- show service-profile

# set service-profile keep-initial-vlan

Configures DWL-8220APs managed by the radio profile to leave a roamed user on the VLAN assigned by the switch where the user logged on. When this option is disabled, a user's VLAN is reassigned by each DWS-1008 to which a user roams.

**Syntax: set service-profile** *name* **keep-initial-vlan {enable | disable}**


Download from Www.Somanuals.com. All Manuals Search And Download.

*name* Service profile name.

**enable** Enables radios to leave a roamed user on the same VLAN instead of reassigning the VLAN.

**disable** Configures radios to reassign a roamed user's VLAN.

**Defaults:** This option is disabled by default.

**Access:** Enabled.

**Usage:** Even when this option is enabled, the DWS-1008 to which a user roams (the roamed-to switch) can reassign the VLAN in any of the following cases:

- A location policy on the local switch reassigns the VLAN.
- The user is configured in the switch's local database and the VLAN-Name attribute is set on the user or on a user group the user is in.
- The access rule on the roamed-to switch uses RADIUS, and the VLAN-Name attribute is set on the RADIUS server.

**Examples:** The following command enables the keep-initial-vlan option on service profile *sp3*:

```
DWS-1008# set service-profile sp3 keep-initial-vlan enable
success: change accepted.
```

**See Also:**
- show service-profile

# set service-profile long-retry-count

Changes the long retry threshold for a service profile. The long retry threshold specifies the number of times a radio can send a long unicast frame without receiving an acknowledgment. A long unicast frame is a frame that is equal to or longer than the frag-threshold.

**Syntax: set service-profile** *name* **long-retry-count** *threshold*

*name* Service profile name.

*threshold* Number of times the radio can send the same long unicast frame. You can enter a value from 1 through 15.

**Defaults:** The default long unicast retry threshold is 5 attempts.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Access:** Enabled.

**Usage:** The length of time a client can remain idle (unresponsive to idle-client probes) is specified by the **user-idle-timeout** command.

**Examples:** The following command changes the long retry threshold for service profile *sp1* to 8:

```
DWS-1008# set service-profile sp1 long-retry-count 8
success: change accepted.
```

**See Also:**
- set radio-profile frag-threshold
- set service-profile short-retry-count
- show service-profile

## set service-profile no-broadcast

Disables or reenables the no-broadcast mode. The no-broadcast mode helps reduce traffic overhead on an SSID by leaving more of an SSID's bandwidth available for unicast traffic. The no-broadcast mode also helps VoIP handsets conserve power by reducing the amount of broadcast traffic sent to the phones.

When enabled, the no-broadcast mode prevents AP radios from sending DHCP or ARP broadcasts to clients on the service profile's SSID. Instead, an AP radio handles this traffic as follows:

- ARP requests—If the SSID has clients whose IP addresses the DWL-1008 does not already know, the DWS-1008 allows the DWS-8220AP to send the ARP request as a unicast to only those stations whose addresses the DWS-1008 does not know. The AP does not forward the ARP request as a broadcast and does not send the request as a unicast to stations whose addresses the DWS-1008 already knows.

- DHCP Offers or Acks—If the destination MAC address belongs to a client on the SSID, the AP sends the DHCP Offer or Ack as a unicast to that client only.

The no-broadcast mode does not affect other types of broadcast traffic and does not prevent clients from sending broadcasts.

**Syntax: set service-profile** *name* **no-broadcast {enable | disable}**


Download from Www.Somanuals.com. All Manuals Search And Download.

*name* Service profile name.

**enable** Enables the no-broadcast mode. APs are not allowed to send broadcast traffic to clients on the service profile's SSID.

**disable** Disables the no-broadcast mode.

**Defaults:** The no-broadcast mode is disabled by default. (Broadcast traffic not disabled.)

**Access:** Enabled.

**Usage:** To further reduce ARP traffic on a service profile, use the **set service-profile proxy-arp** command to enable Proxy ARP.

**Examples:** The following command enables the no-broadcast mode on service profile *sp1*:

```
DWS-1008# set service-profile sp1 no-broadcast enable
success: change accepted.
```

**See Also:**
- set service-profile dhcp-restrict
- set service-profile proxy-arp
- show service-profile

# set service-profile proxy-arp

Enables proxy ARP. When proxy ARP is enabled, the DWS-1008 replies to ARP requests for client IP address on behalf of the clients. This feature reduces broadcast overhead on a service profile's SSID by eliminating ARP broadcasts from APs to the SSID's clients.

If the ARP request is for a client whose IP address the DWS-1008 does not already know, the DWS-1008 allows DWL-8220Aps to send the ARP request to clients. If the no-broadcast mode is also enabled, the APs send the ARP request as a unicast to only the clients whose addresses the DWS-1008 does not know. However, if no-broadcast mode is disabled, the APs sends the ARP request as a broadcast to all clients on the SSID.

**Syntax: set service-profile** *name* **proxy-arp {enable | disable}**

*name* Service profile name.

**enable** Enables proxy ARP.

**disable** Disables proxy ARP.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** Proxy ARP is disabled by default.

**Access:** Enabled.

**Usage:** To further reduce broadcast traffic on a service profile, use the set service-profile no-broadcast command to disable DHCP and ARP request broadcasts.

**Examples:** The following command enables proxy ARP on service profile *sp1*:

```
DWS-1008# set service-profile sp1 proxy-arp enable
success: change accepted.
```

**See Also:**
- set service-profile dhcp-restrict
- set service-profile no-broadcast
- show service-profile

## set service-profile psk-phrase

Configures a passphrase for preshared key (PSK) authentication to use for authenticating WPA clients, in a service profile. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

**Syntax: set service-profile** *name* **psk-phrase** *passphrase*

*name* Service profile name.

*passphrase* An ASCII string from 8 to 63 characters long. The string can contain blanks if you use quotation marks at the beginning and end of the string.

**Defaults:** None.

**Access:** Enabled.

**Usage:** MSS converts the passphrase into a 256-bit binary number for system use and a raw hexadecimal key to store in the DWS-1008's configuration. Neither the binary number nor the passphrase itself is ever displayed in the configuration.

To use PSK authentication, you must enable it and you also must enable the WPA IE.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command configures service profile sp3 to use passphrase "1234567890123<>?=+&% The quick brown fox jumps over the lazy sl":

```
DWS-1008# set service-profile sp3 psk-phrase "1234567890123<>?=+&% The
quick brown fox jumps over the lazy sl"
success: change accepted.
```

**See Also:**
- set mac-user attr
- set service-profile auth-psk
- set service-profile psk-raw
- set service-profile wpa-ie
- show service-profile

# set service-profile psk-raw

Configures a raw hexadecimal preshared key (PSK) to use for authenticating WPA clients, in a service profile. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

**Syntax: set service-profile** *name* **psk-raw** *hex*

| | |
|---|---|
| *name* | Service profile name. |
| *hex* | A 64-bit ASCII string representing a 32-digit hexadecimal number. Enter the two-character ASCII form of each hexadecimal number. |

**Defaults** None.

**Access:** Enabled.

**Usage:** MSS converts the hexadecimal number into a 256-bit binary number for system use. MSS also stores the hexadecimal key in the DWS-1008's configuration. The binary number is never displayed in the configuration.

To use PSK authentication, you must enable it and you also must enable the WPA IE.

**Examples:** The following command configures service profile *sp3* to use a raw PSK with PSK clients:

```
DWS-1008# set service-profile sp3 psk-raw
c25d3fe4483e867d1df96eaacdf8b02451fa0836162e758100f5f6b87965e59d
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile rsn-ie

Enables the Robust Security Network (RSN) Information Element (IE).

The RSN IE advertises the RSN (sometimes called WPA2) authentication methods and cipher suites supported by radios in the radio profile mapped to the service profile.

**Syntax: set service-profile** *name* **rsn-ie {enable | disable}**

| | |
|---|---|
| *name* | Service profile name. |
| **enable** | Enables the RSN IE. |
| **disable** | Disables the RSN IE. |

**Defaults:** The RSN IE is disabled by default.

**Access:** Enabled.

**Usage:** When the RSN IE is enabled, the default authentication method is 802.1X. There is no default cipher suite. You must enable the cipher suites you want the radios to support.

**Examples:** The following command enables the RSN IE in service profile *sprsn*:

```
DWS-1008# set service-profile sprsn rsn-ie enable
success: change accepted.
```

**See Also:**
- set service-profile auth-dot1x
- set service-profile auth-psk
- set service-profile cipher-ccmp
- set service-profile cipher-wep104
- set service-profile cipher-wep40
- show service-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile shared-key-auth

Enables shared-key authentication, in a service profile.

**Note.** Use this command only if advised to do so by D-Link. This command does not enable preshared key (PSK) authentication for Wi-Fi Protected Access (WPA). To enable PSK encryption for WPA, use the set service-profile auth-psk command.

**Syntax: set service-profile** *name* **shared-key-auth {enable | disable}**

*name* Service profile name.

**enable** Enables shared-key authentication.

**disable** Disables shared-key authentication.

**Defaults:** Shared-key authentication is disabled by default.

**Access:** Enabled.

**Usage:** Shared-key authentication is supported only for encrypted SSIDs. In addition, if you enable shared-key authentication, RSN, WPA, TKIP, and CCMP must be disabled. By default, RSN, WPA, and CCMP are already disabled, but TKIP is enabled; you must manually disable TKIP. To disable TKIP, use the set service-profile cipher-tkip disable command.

**Examples:** The following command enables shared-key authentication in service profile *sp4*:

```
DWS-1008# set service-profile sp4 shared-key-auth enable
success: change accepted.
```

**See Also:**
- set radio-profile mode
- set service-profile cipher-tkip
- show service-profile

# set service-profile short-retry-count

Changes the short retry threshold for a service profile. The short retry threshold specifies the number of times a radio can send a short unicast frame without receiving an acknowledgment. A short unicast frame is a frame that is shorter than the frag-threshold.

**Syntax: set service-profile** *name* **short-retry-count** *threshold*


Download from Www.Somanuals.com. All Manuals Search And Download.

*name* Service profile name.

*threshold* Number of times a radio can send the same short unicast frame. You can enter a value from 1 through 15.

**Defaults:** The default short unicast retry threshold is 5 attempts.

**Access:** Enabled.

**Examples:** The following command changes the short retry threshold for service profile *sp1* to 3:

```
DWS-1008# set service-profile sp1 short-retry-count 3
success: change accepted.
```

**See Also:**
- set radio-profile frag-threshold
- set service-profile long-retry-count o
- show service-profile

# set service-profile soda agent-directory

Specifies the directory on the DWL-1008 switch where the SODA agent files for a service profile are located.

**Syntax: set service-profile** *name* **soda agent-directory** *directory*

*name* Service profile name.

*directory* Directory on the DWS-1008 for SODA agent files.

**Defaults:** By default, the DWS-1008 expects SODA agent files to be located in a directory with the same name as the service profile.

**Access:** Enabled.

**Usage:** If the same SODA agent is used for multiple service profiles, you can use this command to specify a single directory for SODA agent files on the DWS-1008, rather than placing the same SODA agent files in a separate directory for each service profile.

**Examples:** The following command specifies soda-agent as the location for SODA agent files for service profile *sp1*:

```
DWS-1008# set service-profile sp1 soda agent-directory soda-agent
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile soda enforce-checks

Specifies whether a client is allowed access to the network after it has downloaded and run the SODA agent security checks.

**Syntax: set service-profile** *name* **enforce-checks {enable | disable}**

*name* Service profile name.

**enable** SODA agent checks are performed before the client is allowed access to the network.

**disable** Allows the client access to the network immediately after the SODA agent is downloaded, without waiting for the checks to be run.

**Defaults:** By default, SODA agent checks are performed before the client is allowed access to the network.

**Access:** Enabled.

**Usage:** When the SODA agent is enabled in a service profile, by default the SODA agent checks are downloaded to a client and run before the client is allowed on the network. You can use this command to disable the enforcement of the SODA security checks, so that the client is allowed access to the network immediately after the SODA agent is downloaded, rather than waiting for the security checks to be run.

When the enforce checks option is enabled, upon successful completion of the SODA agent checks, the client performs an HTTP Get operation to load the success page. Upon loading the success page, the client is granted access to the network.

In order for the client to load the success page, you must make sure the SODA agent is configured (through SODA Manager) with the correct URL of the success page, so that the DWS-1008 can serve the page to the client.

Similarly, you must make sure the SODA agent is configured with the correct URLs of the failure and logout pages, so that when the client requests these pages, the DWS-1008 can serve those pages as well.

**Examples:** The following command allows network access to clients after they have downloaded the SODA agent, but without requiring that the SODA agent checks be completed:

```
DWS-1008# set service-profile sp1 enforce-checks disable
success: change accepted.
```

**See Also:**

- set service-profile soda mode



Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile soda failure-page

Specifies a page on the DWS-1008 that is loaded when a client fails the security checks performed by the SODA agent.

**Syntax: set service-profile** *name* **soda failure-page** *page*

*name* Service profile name.

*page* Page that is loaded if the client fails the security checks performed by the SODA agent.

**Defaults:** By default, the DWS-1008 dynamically generates a page indicating that the SODA agent checks have failed.

**Access:** Enabled.

**Usage:** Use this command to specify a custom page that is loaded by the client when the SODA agent checks fail. After this page is loaded, the specified remediation ACL takes effect, or if there is no remediation ACL configured, then the client is disconnected from the network.

This functionality occurs only when the enforce checks option is enabled for the service profile. The enforce checks option is enabled by default.

The page is assumed to reside in the root directory on the DWS-1008. You can optionally specify a different directory where the page resides.

**Examples:** The following command specifies *failure.html* as the page to load when a client fails the SODA agent checks:

```
DWS-1008# set service-profile sp1 soda failure-page failure.html
success: change accepted.
```

The following command specifies *failure.html*, in the soda-files directory, as the page to load when a client fails the SODA agent checks:

```
DWS-1008# set service-profile sp1 soda failure-page soda-files/failure.html
success: change accepted.
```

**See Also:**
- set service-profile soda enforce-checks
- set service-profile soda remediation-acl
- show service-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile soda logout-page

Specifies a page on the DWS-1008 that is loaded when a client logs out of the network by closing the SODA virtual desktop.

**Syntax: set service-profile** *name* **soda logout-page** *page*

*name* Service profile name.

*page* Page that is loaded when the client closes the SODA virtual desktop.

**Defaults:** None.

**Access:** Enabled.

**Usage:** When a client closes the SODA virtual desktop, the client is automatically disconnected from the network. You can use this command to specify a page that is loaded when the client closes the SODA virtual desktop.

The client can request this page at any time, to ensure that the client's session has been terminated. You can add the IP address of the DWS-1008 to the DNS server as a well-known name, and you can advertise the URL of the page to users as a logout page.

The page is assumed to reside in the root directory on the DWS-1008. You can optionally specify a different directory where the page resides.

Note that you must also enable the HTTPS server on the DWS-1008, so that clients can log out of the network and access the logout page using HTTPS. To do this, use the set ip https server enable command.

**Examples:** The following command specifies *logout.html* as the page to load when a client closes the SODA virtual desktop:

```
DWS-1008# set service-profile sp1 soda logout-page logout.html
success: change accepted.
```

The following command specifies logout.html, in the soda-files directory, as the page to load when a client closes the SODA virtual desktop:

```
DWS-1008# set service-profile sp1 soda logout-page soda-files/logout.html
success: change accepted.
```

**See Also:**
- set ip https server
- show service-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile soda mode

Enables or disables Sygate On-Demand (SODA) functionality for a service profile.

**Syntax: set service-profile** *name* **soda mode {enable | disable}**

*name* Service profile name.

**enable** Enables SODA functionality for the service profile.

**disable** Disables SODA functionality for the service profile.

**Defaults:** Disabled.

**Access:** Enabled.

**Usage:** When SODA functionality is enabled for a service profile, a SODA agent is downloaded to clients attempting to connect to an AP managed by the service profile. The SODA agent performs a series of security-related checks on the client; if the client passes the checks, it can be admitted to the network.

SODA functionality requires that Web Portal WebAAA also be enabled for the service profile.

**Examples:** The following command enables SODA functionality for service profile *sp1*:

```
DWS-1008# set service-profile sp1 soda mode enable
success: change accepted.
```

**See Also:**
- install soda agent
- set service-profile soda enforce-checks
- show service-profile

# set service-profile soda remediation-acl

Specifies an ACL to be applied to a client if it fails the checks performed by the SODA agent.

**Syntax: set service-profile** *name* **soda remediation-acl** *acl-name*

*name* Service profile name.

*acl-name* Name of an existing security ACL to use as a remediation ACL for this service profile. ACL names must start with a letter and are case-insensitive.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** Disabled.

**Access:** Enabled.

**Usage:** If the SODA agent checks fail on a client, by default the client is disconnected from the network. Optionally, you can specify a failure page for the client to load (with the set service-profile soda failure-page command). When the failure page is loaded, you can optionally specify a remediation ACL to apply to the client. The remediation ACL can be used to grant the client limited access to network resources, for example. If there is no remediation ACL configured, then the client is disconnected from the network when the failure page is loaded.

This functionality occurs only when the enforce checks option is enabled for the service profile. The enforce checks option is enabled by default.

**Examples:** The following command configures the DWS-1008 to apply *acl-1* to a client when it loads the failure page:

```
DWS-1008# set service-profile sp1 soda remediation-acl acl-1
success: change accepted.
```

**See Also:**
- set service-profile soda enforce-checks
- set service-profile soda failure-page
- show service-profile

## set service-profile soda success-page

Specifies a page on the DWL-1008 switch that is loaded when a client passes the security checks performed by the SODA agent.

**Syntax: set service-profile** *name* **soda success-page** *page*

| | |
|---|---|
| *name* | Service profile name. |
| *page* | Page that is loaded if the client passes the security checks performed by the SODA agent. |

**Defaults:** By default, the DWL-1008 switch generates a page indicating that the client passed the SODA agent checks.

**Access:** Enabled.

**Usage:** Use this command to specify a custom page that is loaded by the client when it passes the checks performed by the SODA agent. After this page is loaded, the client is placed in its assigned VLAN and granted access to the network.


Download from Www.Somanuals.com. All Manuals Search And Download.

The page is assumed to reside in the root directory on the DWS-1008. optionally specify a different directory where the page resides.

This functionality occurs only when the enforce checks option is enabled for the service profile. The enforce checks option is enabled by default.

**Examples:** The following command specifies *success.html*, which resides in the root directory on the DWS-1008, as the page to load when a client passes the SODA agent checks:

```
DWS-1008# set service-profile sp1 soda success-page success.html
success: change accepted.
```

The following command specifies *success.html*, which resides in the soda-files directory on the DWS-1008, as the page to load when a client passes the SODA agent checks:

```
DWS-1008# set service-profile sp1 soda success-page soda-files/success.html
success: change accepted.
```

**See Also:**
- set service-profile soda enforce-checks
- set service-profile soda mode
- show service-profile

# set service-profile ssid-name

Configures the SSID name in a service profile.

**Syntax: set service-profile** *name* **ssid-name** *ssid-name*

| | |
|---|---|
| *name* | Service profile name. |
| *ssid-name* | Name of up to 32 alphanumeric characters. You can include blank spaces in the name, if you delimit the name with single or double quotation marks. You must use the same type of quotation mark (either single or double) on both ends of the string. |

**Defaults:** The default SSID type is crypto (encrypted) and the default name is *dlink*.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command applies the name *guest* to the SSID managed by service profile *clear_wlan*:

```
DWS-1008# set service-profile clear_wlan ssid-name guest
success: change accepted.
```

The following command applies the name *corporate users* to the SSID managed by service profile *mycorp_srvcprf*:

```
DWS-1008# set service-profile mycorp_srvcprf ssid-name "corporate users"
success: change accepted.
```

**See Also:**
- set service-profile ssid-type
- show service-profile

# set service-profile ssid-type

Specifies whether the SSID managed by a service profile is encrypted or unencrypted.

**Syntax: set service-profile** *name* **ssid-type [clear | crypto]**

| | |
|---|---|
| *name* | Service profile name. |
| **clear** | Wireless traffic for the service profile's SSID is not encrypted. |
| **crypto** | Wireless traffic for the service profile's SSID is encrypted. |

**Defaults:** The default SSID type is crypto.

**Access:** Enabled.

**Examples:** The following command changes the SSID type for service profile *clear_wlan* to **clear**:

```
DWS-1008# set service-profile clear_wlan ssid-type clear
success: change accepted.
```

**See Also:**
- set service-profile ssid-name
- show service-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile static-cos

Enables or disables static CoS on a service profile. Static CoS assigns the same CoS level to all traffic on the service profile's SSID, regardless of 802.1p or DSCP markings in the packets themselves, and regardless of any ACLs that mark CoS. This option provides a simple way to configure an SSID for priority traffic such as VoIP traffic.

When static CoS is enabled, the standard MSS prioritization mechanism is not used. Instead, the AP sets CoS as follows:

- For traffic from the AP to clients, the AP places the traffic into the forwarding queue that corresponds to the CoS level configured on the service profile. For example, if the static CoS level is set to 7, the AP radio places client traffic in its Voice queue.
- For traffic from clients to the network, the AP marks the DSCP value in the IP headers of the tunnel packets used to carry the user data from the AP to the DWS-1008.

**Syntax: set service-profile** *name* **static-cos {enable | disable}**

| | |
|---|---|
| *name* | Service profile name. |
| **enable** | Enables static CoS on the service profile. |
| **disable** | Disables static CoS on the service profile. |

**Defaults:** Static CoS is disabled by default.

**Access:** Enabled.

**Usage:** The CoS level is specified by the set service-profile cos command.

**Examples:** The following command enables static CoS on service profile *sp1*:

```
DWS-1008# set service-profile sp1 static-cos enable
success: change accepted.
```

**See Also:**
- set service-profile cos
- show service-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile tkip-mc-time

Changes the length of time that AP radios use countermeasures if two message integrity code (MIC) failures occur within 60 seconds. When countermeasures are in effect, DWL-8220APs dissociate all TKIP and WPA WEP clients and refuse all association and reassociation requests until the countermeasures end.

**Syntax: set service-profile** *name* **tkip-mc-time** *wait-time*

*name* Service profile name.

*wait-time* Number of milliseconds (ms) countermeasures remain in effect. You can specify from 0 to 60,000.

**Defaults:** The default countermeasures wait time is 60,000 ms (60 seconds).

**Access:** Enabled.

**Usage:** Countermeasures apply only to TKIP and WEP clients. This includes WPA WEP clients and non-WPA WEP clients. CCMP clients are not affected.

The TKIP cipher suite must be enabled. The WPA IE also must be enabled.

**Examples:** The following command changes the countermeasures wait time for service profile *sp3* to 30,000 ms (30 seconds):

```
DWS-1008# set service-profile sp3 tkip-mc-time 30000
success: change accepted.
```

**See Also:**
- set service-profile cipher-tkip
- set service-profile wpa-ie
- show service-profile

# set service-profile transmit-rates

Changes the data rates supported by DWL-8220APs for a service-profile's SSID.

**Syntax: set service-profile** *name* **transmit-rates {11a | 11b | 11g} mandatory** *rate-list* **[disabled** *rate-list***] [beacon-rate** *rate***] [multicast-rate {***rate* **| auto}]**


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| *name* | Service profile name. |
| **11a \| 11b \| 11g** | Radio type. |
| **mandantory** *rate-list* | Set of data transmission rates that clients are required to support in order to associate with an SSID on an AP. A client must support at least one of the mandatory rates.<br><br>These rates are advertised in the basic rate set of 802.11 beacons, probe responses, and reassociation response frames sent by AP radios.<br><br>Data frames and management frames sent by APs use one of the specified mandatory rates. The valid rates depend on the radio type:<br><br>• **11a** - 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0<br>• **11b** - 1.0, 2.0, 5.5, 11.0<br>• **11g**- 1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0<br><br>Use a comma to separate multiple rates; for example: **6.0,9.0,12.0** |
| **disabled** *rate-list* | Data transmission rates that APs will not use to transmit data. This setting applies only to data sent by the APs. The radios will still accept frames from clients at disabled data rates.<br><br>The valid rates depend on the radio type and are the same as the valid rates for **mandatory**. |
| **beacon-rate** *rate* | Data rate of beacon frames sent by APs. This rate is also used for probe-response frames. |
| **multicast-rate {***rate* **\| auto}** | The valid rates depend on the radio type and are the same as the valid rates for **mandatory**. However, you cannot set the beacon rate to a disabled rate.<br><br>Data rate of multicast frames sent by APs.<br><br>• *rate* - Sets the multicast rate to a specific rate. The valid rates depend on the radio type and are the same as the valid rates for mandatory. However, you cannot set the multicast rate to a disabled rate.<br><br>• **auto** - Sets the multicast rate to the highest rate that can reach all clients connected to the AP. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** This command has the following defaults:

- **mandantory:**
  - 11a **- 6.0,12.0,24.0**
  - 11b **- 1.0,2.0**
  - 11g **- 1.0,2.0,5.5,11.0**

- **disabled -** None. All rates applicable to the radio type are supported by default.

- **beacon-rate:**
  - 11a **- 6.0**
  - 11b **- 2.0**
  - 11g **- 2.0**

- **multicast-rate - auto** for all radio types.

**Access:** Enabled.

**Usage:** If you disable a rate, you cannot use the rate as a mandatory rate or the beacon or multicast rate. All rates that are applicable to the radio type and that are not disabled are supported by the radio.

The TKIP cipher suite must be enabled. The WPA IE also must be enabled.

**Examples:** The following command sets 802.11a mandatory rates for service profile *sp1* to 6 Mbps and 9 Mbps, disables rates 48 Mbps and 54 Mbps, and changes the beacon rate to 9 Mbps:

```
DWS-1008# set service-profile sp1 transmit-rates 11a mandatory 6.0,9.0 disabled
48.0,54.0 beacon-rate 9.0
success: change accepted.
```

**See Also:**
- show service-profile

# set service-profile user-idle-timeout

Changes the number of seconds MSS will leave a session up for a client that is not sending data and is not responding to keepalives (idle-client probes). If the timer expires, the client's session is changed to the Dissociated state.

The timer is reset to 0 each time a client sends data or responds to an idle-client probe. If the idle-client probe is disabled, the timer is reset each time the client sends data.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Syntax: set service-profile** *name* **user-idle-timeout** *seconds*

*name* Service profile name.

*seconds* Number of seconds a client is allowed to remain idle before MSS changes the session to the Dissociated state. You can specify from 20 to 86400 seconds. To disable the timer, specify 0.

**Defaults:** The default user idle timeout is 180 seconds (3 minutes).

**Access:** Enabled.

**Examples:** The following command increases the user idle timeout to 360 seconds (6 minutes):

```
DWS-1008# set service-profile sp1 user-idle-timeout 360
success: change accepted.
```

**See Also:**
- set service-profile idle-client-probing
- set service-profile web-portal-session-timeout
- show service-profile

# set service-profile web-portal-acl

Changes the ACL name MSS uses to filter a Web-Portal user's traffic during authentication.

Use this command if you create a custom Web-Portal ACL to allow more than just DHCP traffic during authentication. For example, if you configure an ACL that allows a Web-Portal user to access a credit card server, use this command to use the custom ACL for Web-Portal users that associate with the service profile's SSID.

**Syntax: set service-profile** *name* **web-portal-acl** *aclname*

*name* Service profile name.

*aclname* Name of the ACL to use for filtering Web-Portal user traffic during authentication.

**Defaults:** By default, a service profile's **web-portal-acl** option is unset. However,when you change the service profile's **auth-fallthru** option to **web-portal**, MSSsets the **web-portal-acl** option to *portalacl*. (MSS automatically creates the *portalacl* ACL the first time you set any service profile's **auth-fallthru** option to **web-portal**.)


Download from Www.Somanuals.com. All Manuals Search And Download.

**Access:** Enabled.

**Usage:** The first time you set the service profile's **auth-fallthru** option to **web-portal**, MSS sets the **web-portal-acl** option to *portalacl*. The value remains *portalacl* even if you change the **auth-fallthru** option again. To change the **web-portal-acl** value, you must use the **set service-profile web-portal-acl** command.

The Web-Portal ACL applies only to users who log on using Web-Portal, and applies only during authentication. After a Web-Portal user is authenticated, the Web-Portal ACL no longer applies. ACLs and other user attributes assigned to the username are applied instead.

**Examples:** The following command changes the Web-Portal ACL name to on service profile *sp3* to *creditsrvr*:

```
DWS-1008# set service-profile sp3 web-portal-acl creditsrvr
success: change accepted.
```

**See Also:**
- set service-profile auth-fallthru
- show service-profile

# set service-profile web-portal-form

Specifies a custom login page to serve to WebAAA users who request the SSID managed by the service profile.

**Syntax: set service-profile** *name* **web-portal-form** *url*

| | |
|---|---|
| *name* | Service profile name. |
| *url* | DWS-1008 subdirectory name and HTML page name of the login page. Specify the full path. For example, *corpa-ssid/corpa.html*. |

**Defaults:** The D-Link Web login page is served by default.

**Access:** Enabled.

**Usage:** D-link recommends that you create a subdirectory for the custom page and place all the page's files in that subdirectory. Do not place the custom page in the root directory of the switch's user file area.

If the custom login page includes gif or jpg images, their path names are interpreted relative to the directory from which the page is served.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Note:** To use WebAAA, the fallthru authentication type in the service profile that manages the SSID must be set to web-portal. To use WebAAA for a wired authentication port, edit the port configuration with the set port type wired-auth command.

The web-portal authentication type also requires additional configuration items.

**Examples:** The following commands create a subdirectory named *corpa*, copy a custom login page named *corpa-login.html* and a jpg image named *corpa-logo.jpg* into that subdirectory, and set the Web login page for service profile *corpa-service* to *corpa-login.html*:

```
DWS-1008# mkdir corpa
success: change accepted.

DWS-1008# copy tftp://10.1.1.1/corpa-login.html corpa/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]

DWS-1008# copy tftp://10.1.1.1/corpa-logo.jpg corpa/corpa-logo.jpg
success: received 1202 bytes in 0.402 seconds [ 2112 bytes/sec]

DWS-1008# dir corpa
================================================================
file:
Filename                                  Size          Created
file:corpa-login.html                     637 bytes     Aug 12 2004, 15:42:26
file:corpa-logo.jpg                       1202 bytes    Aug 12 2004, 15:57:11
Total:          1839 bytes used, 206577 Kbytes free

DWS-1008# set service-profile corpa-service web-portal-form
corpa/corpa-login html
success: change accepted.
```

**See Also:**

- copy
- dir
- mkdir
- set port type wired-auth
- set service-profile auth-fallthru
- set web-portal
- show service-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile web-portal-session-timeout

Changes the number of seconds MSS allows Web Portal WebAAA sessions to remain in the Deassociated state before being terminated automatically.

**Syntax: set service-profile** *name* **web-portal-session-timeout** *seconds*

*name* Service profile name.

*seconds* Number of seconds MSS allows Web Portal WebAAA sessions to remain in the Deassociated state before being terminated automatically. You can specify from 5 to 2800 seconds.

**Defaults:** The default Web Portal WebAAA session timeout is 5 seconds.

**Access:** Enabled.

**Usage:** When a client that has connected through Web Portal WebAAA enters standby or hibernation mode, the client may be idle for longer than the User idle-timeout period. When the User idle-timeout period expires, MSS places the client's Web Portal WebAAA session in the Deassociated state. The Web Portal WebAAA session can remain in the Deassociated state for a configurable amount of time before being terminated automatically. This configurable amount of time is called the Web Portal WebAAA session timeout period. You can use this command to set the number of seconds in the Web Portal WebAAA session timeout period.

Note that the Web Portal WebAAA session timeout period applies only to Web Portal WebAAA sessions already authenticated with a username and password. For all other Web Portal WebAAA sessions, the default Web Portal WebAAA session timeout period of 5 seconds is used.

**Examples:** The following command allows Web Portal WebAAA sessions to remain in the Deassociated state 180 seconds before being terminated automatically.

```
DWS-1008# set service-profile sp1 web-portal-session-timeout 180
success: change accepted.
```

**See Also:**
- set service-profile user-idle-timeout
- show service-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# set service-profile wep active-multicast-index

Specifies the static Wired-Equivalent Privacy (WEP) key (one of four) to use for encrypting multicast frames.

**Syntax: set service-profile** *name* **wep active-multicast-index** *num*

*name* Service profile name.

*num* WEP key number. You can enter a value from 1 through 4.

**Defaults:** If WEP encryption is enabled and WEP keys are defined, APs use WEP key 1 to encrypt multicast frames, by default.

**Access:** Enabled.

**Usage:** Before using this command, you must configure values for the WEP keys you plan to use. Use the **set service-profile wep key-index** command.

**Examples:** The following command configures service profile sp2 to use WEP key 2 for encrypting multicast traffic:

```
DWS-1008# set service-profile sp2 wep active-multicast-index 2
success: change accepted.
```

**See Also:**
- set service-profile wep active-unicast-index
- set service-profile wep key-index
- show service-profile

# set service-profile wep active-unicast-index

Specifies the static Wired-Equivalent Privacy (WEP) key (one of four) to use for encrypting unicast frames.

**Syntax: set service-profile** name **wep active-unicast-index** num

*name* Service profile name.

*num* WEP key number. You can enter a value from 1 through 4.

**Defaults:** If WEP encryption is enabled and WEP keys are defined, APs use WEP key 1 to encrypt unicast frames, by default.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Access:** Enabled.

**Usage:** Before using this command, you must configure values for the WEP keys you plan to use. Use the set service-profile wep key-index command.

**Examples:** The following command configures service profile sp2 to use WEP key 4 for encrypting unicast traffic:

```
DWS-1008# set service-profile sp2 wep active-unicast-index 4
success: change accepted.
```

**See Also:**
- set service-profile wep active-multicast-index
- set service-profile wep key-index
- show service-profile

# set service-profile wep key-index

Sets the value of one of four static Wired-Equivalent Privacy (WEP) keys for static WEP encryption.

**Syntax: Syntax set service-profile** *name* **wep key-index** *num* **key** *value*

| | |
|---|---|
| *name* | Service profile name. |
| **key-index** *num* | WEP key index. You can enter a value from 1 through 4. |
| **key** *value* | Hexadecimal value of the key. You can enter a 10-character ASCII string representing a 5-byte hexadecimal number or a 26-character ASCII string representing a 13-byte hexadecimal number. You can use numbers or letters. ASCII characters in the following ranges are supported:<br>• 0 to 9<br>• A to F<br>• a to f |

**Defaults:** By default, no static WEP keys are defined.

**Access:** Enabled.

**Usage:** MSS automatically enables static WEP when you define a WEP key. MSS continues to support dynamic WEP.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command configures a 5-byte WEP key for key index 1 on service profile *sp2* to *aabbccddee*:

```
DWS-1008# set service-profile sp2 wep key-index 1 key aabbccddee
success: change accepted.
```

**See Also:**
- set service-profile wep active-multicast-index
- set service-profile wep active-unicast-index
- show service-profile

# set service-profile wpa-ie

Enables the WPA information element (IE) in wireless frames. The WPA IE advertises the WPA authentication methods and cipher suites supported by radios in the radio profile mapped to the service profile.

**Syntax: set service-profile** *name* **wpa-ie {enable | disable}**

| | |
|---|---|
| *name* | Service profile name. |
| **enable** | Enables the WPA IE. |
| **disable** | Disables the WPA IE. |

**Defaults:** The WPA IE is disabled by default.

**Access:** Enabled.

**Usage:** When the WPA IE is enabled, the default authentication method is 802.1X. There is no default cipher suite. You must enable the cipher suites you want the radios to support.

**Examples:** The following command enables the WPA IE in service profile *sp2*:

```
DWS-1008# set service-profile sp2 wpa-ie enable
success: change accepted.
```

**See Also:**
- set service-profile auth-dot1x
- set service-profile cipher-tkip
- show service-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# show {ap | dap} config

Displays global and radio-specific settings for a DWL-8220AP access point.

**Syntax: show ap config [***port-list* **[radio {1 | 2}]]**

**Syntax: show dap config [***dap-num* **[radio {1 | 2}]]**

| | |
|---|---|
| *port-list* | List of ports connected to the DWL-8220AP access point(s) for which to display configuration settings. |
| *dap-num* | Number of a Distributed AP for which to display configuration settings. |
| **radio 1** | Shows configuration information for radio 1. |
| **radio 2** | Shows configuration information for radio 2. (This option does not apply to single-radio models.) |

**Defaults:** None.

**Access:** Enabled.

**Usage:** MSS lists information separately for each DWL-8220AP access point.

**Examples:** The following example shows configuration information for a DWL-8220AP access point on port 2:

```
DWS-1008# show ap config 2
Port 2: AP model: DWL-8220AP, POE: enable, bias: high, name: DWL-8220AP02
boot-download-enable: YES force-image-download: NO load balancing group: none
location: The conference room contact: Bob the IT guy
Radio 1: type: 802.11g, mode: disabled, channel: 6 tx pwr: 1, profile: default auto-tune
max-power: default
Radio 2: type: 802.11a, mode: disabled, channel: 36 tx pwr: 1, profile: default
auto-tune max-power: default
```

The following example shows configuration information for a Distributed AP access point configured on connection 1:

```
DWS-1008# show dap config 1
Dap 1: serial-id: 12345678, AP model: DWL-8220AP, bias: high, name: DAP01
fingerprint: b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3 boot-download-enable:
YES
force-image-download: NO  load balancing group: none
location: The conference room contact: Bob the IT guy
Radio 1: type: 802.11g, mode: disabled, channel: 6 tx pwr: 1, profile: default
auto-tune max-power: default
Radio 2: type: 802.11a, mode: disabled, channel: 36 tx pwr: 1, profile: default
auto-tune max-power: default
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The following Table describes the fields in this display.

| Field | Description |
|---|---|
| port | DWS-1008 port number.<br><br>**Note:** This field is applicable only if the DWL-8220AP is directly connected to the DWS-1008 and the DWS-1008's port is configured as an AP access port. |
| DAP | Connection ID for the Distributed AP.<br><br>This field is applicable only if the AP is configured on the DWS-1008 as a Distributed AP. |
| serial-id | Serial ID of the DWL-8220AP access point.<br><br>**Note:** This field is displayed only for Distributed APs. |
| AP Model | Access point mdel number. |
| POE | PoE state on the DWS-1008 port:<br>• Enable<br>• Disable |
| name | DWL-8220AP access point name. |
| fingerprint | Hexadecimal fingerprint of the AP's public encryption key.<br><br>**Note:** This field is displayed only for Distributed APs. If the field is blank, the key has not been verified yet by an administrator. |
| boot-download-enable | State of the firmware upgrade option:<br>• YES (automatic upgrades are enabled)<br>• NO (automatic upgrades are disabled) |
| force-image-download | State of the option to force the AP to download a new image:<br>• YES (automatic upgrades are enabled)<br>• NO (automatic upgrades are disabled) |
| load balancing group | Names of the AP load-balancing groups to which the DWL-8220AP access point belongs. If the value is None, the access point does not belong to any load balancing groups. |
| location | Location information for the AP. |
| contact | Contact information for the AP. |
| Radio | Radio number. The information listed below this field applies specifically to the radio. |
| type | Radio type:<br>• 802.11a<br>• 802.11b<br>• 802.11g |
| channel | Channel number. |
| antennatype | External antenna model, if applicable. |
| tx pwr | Transmit power, in dBm. |
| profile | Radio profile that manages the radio. Until you assign the radio to a radio profile, MSS, assigns the radio to the default radio profile. |
| auto-tune max-power | Maximu power level the RF Auto-Tuning feature can set on the radio:<br>• The value *default* means RF Auto-Tuning can set the power up to the maximum level allowed for the country of operation.<br>• A specific numeric value means you or another administrator set the maximum value. |


Download from Www.Somanuals.com. All Manuals Search And Download.

# show {ap | dap} counters

Displays DWL-8220AP access point and radio statistics counters.

**Syntax: show ap counters [***port-list* **[radio {1 | 2}]]**

**Syntax: show dap counters [***dap-num* **[radio {1 | 2}]]**

| | |
|---|---|
| *port-list* | List of ports connected to the DWL-8220AP access point(s) for which to display statistics counters. |
| *dap-num* | Number of a Distributed AP for which to display statistics counters. |
| **radio 1** | Shows statistics counters for radio 1. |
| **radio 2** | Shows statistics counters for radio 2. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** To display statistics counters and other information for individual user sessions, use the **show sessions network** command.

**Examples:** The following command shows statistics counters for Distributed AP 7:

```
DWS-1008# show dap counters 7
DAP: 7 r                    adio: 1
=================================
LastPktXferRate             2          PktTxCount                73473
NumCntInPwrSave             0          MultiPktDrop          0
LastPktRxSigStrength        -89        MultiBytDrop              0
LastPktSigNoiseRatio        4          User Sessions             0
TKIP Pkt Transfer Ct        0          MIC Error Ct              0
TKIP Pkt Replays            0          TKIP Decrypt Err          0
CCMP Pkt Decrypt Err        0          CCMP Pkt Replays          0
CCMP Pkt Transfer Ct        0          RadioResets           0
Radio Recv Phy Err Ct       0          Transmit Retries          60501
Radio Adjusted Tx Pwr       15         Noise Floor               -93
802.3 Packet Tx Ct          0          802.3 Packet Rx Ct        0
No Receive Descriptor       0
```


Download from Www.Somanuals.com. All Manuals Search And Download.

| | TxUniPkt | TxMultiPkt | TxUniByte | TxMultiByte | RxPkt | RxByte | UndcrptPkt | UndcrptByte | PhyErr |
|---|---|---|---|---|---|---|---|---|---|
| 1.0: | 1017 | 0 | 10170 | 0 | 14 | 8347 | 0 | 0 | 3964 |
| 2.0: | 5643 | 55683 | 822545 | 8697520 | 3 | 1670 | 0 | 0 | 8695 |
| 5.5: | 0 | 0 | 0 | 0 | 5 | 258 | 0 | 0 | 4 |
| 6.0: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 51 |
| 9.0: | 0 | 0 | 0 | 0 | 1 | 172 | 0 | 0 | 53 |
| 11.0: | 0 | 0 | 0 | 0 | 17 | 998 | 0 | 0 | 35 |
| 12.0: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 26 |
| 18.0: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 38 |
| 24.0: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 47 |
| 36.0: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 48.0: | 0 | 0 | 0 | 0 | 1 | 68 | 0 | 0 | 29 |
| 54.0: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 5 |
| TOTL: | 6660 | 55683 | 832715 | 8697520 | 41 | 11513 | 0 | 0 | 12948 |

…

The following table describes the fields in this display:

| Field | Description |
|---|---|
| DAP<br><br>Port | Distributed AP number.<br><br>DWS-1008 port number (if the AP is directly connected to the DWS-1008 and the DWS-1008 port is configured as an AP access port). |
| radio | Radio number. |
| LastPktXferRate | Data transmit rate, in Mbps, of the last packet received by the DWL-8220AP access point. |
| NumCntInPwrSave | Number of clients currently in power save mode. |
| LastPktRxSigStrength | Signal strength, in dBm, of the last packet received by the DWL-8220AP access point. |
| LastPktSigNoiseRatio | Signal-to-noise ratio (SNR), in decibels (dB), of the last packet received by the DWL-8220AP access point.<br><br>This value indicates the strength of the radio signal above the noise floor. For example, if the noise floor is -88 and the signal strength is -68, the SNR is 20.<br><br>If the value is below 10, this indicates a weak signal and might indicate a problem in the RF environment. |
| TKIP Pkt Transfer Ct | Total number of TKIP packets sent and received by the radio. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| TKIP Pkt Replays | Number of TKIP packets that were resent to the AP by a client.<br><br>A low value (under about one hundred) does not necessarily indicate a problem. However, if this counter is increasing steadily or has a very high value (in the hundreds or more), a Denial of Service (DoS) attack might be occurring. Contact D-Link Technical Support. |
| CCMP Pkt Decrypt Err | Number of times a decryption error occurred with a packet encrypted with CCMP.<br><br>Occasional decryption errors do not indicate a problem.<br><br>However, steadily increasing errors or a high number of errors can indicate that data loss is occurring in the network. Generally, this is caused by a key mismatch between a client and the AP.<br><br>To locate the client that is experiencing decryption errors (and therefore is likely causing this counter to increment on the AP), use the **show sessions network session-id** *session-id* command for each client on the radio. After you identify the client that is causing the errors, disable and reenable the client (wireless NIC). |
| CCMP Pkt Transfer Ct | Total number of CCMP packets sent and received by the radio. |
| Radio Recv Phy Err Ct | Number of times radar caused packet errors. If this counter increments rapidly, there is a problem in the RF environment.<br><br>**Note:** This counter increments only when radar is detected. Rate-specific Phy errors are instead counted in the PhyError columns for individual data rates. |
| Radio Adjusted Tx Pwr | Current power level set on the radio. If RF Auto-Tuning of power is enabled, this value is the power set by RF Auto-Tuning. If RF Auto-Tuning is disabled, this value is the statically configured power level. |
| 802.3 Packet Tx Ct | Number of raw 802.3 packets transmitted by the radio. These are LocalTalk (AppleTalk) frames. This counter increments only if LocalTalk traffic is present. |
| No Receive Descriptor | Number of packets for which the DWL-8220AP could not create a descriptor. A descriptor describes a received packet's size and its location in AP memory. The AP buffers descriptors, and clears them during<br>interframe spaces.<br><br>This counter increments if the AP runs out of buffers for received packets. This condition can occur when a noise burst temporarily floods the air and the AP attempts to buffer the noise as packets.<br><br>Buffer overruns are normal while an AP is booting. However, if they occur over an extended period of time when the AP is fully active, this can indicate RF interference. |
| PktTxCount | Number of packets transmitted by the radio. |
| MultiPktDrop | Number of multicast packets dropped by the radio due to a buffer overflow on the AP. This counter increments if there is too much multicast traffic or there is a problem with the multicast packets. Normally, this counter should be 0. |
| MultiBytDrop | Number of multicast bytes dropped by the radio due to a buffer overflow on the AP. (See the description for MultiPktDrop.) |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| User Sessions | Number of clients currently associated with the radio.<br><br>Generally, this counter is equal to the number of sessions listed for the radio in show sessions output. However, the counter can differ from the counter in show sessions output if a client is associated with the radio but has not yet completed 802.1X authentication. In this case, the client is counted by this counter but not in the show sessions output.<br><br>Although there is no specific normal range for this counter, a high or low number relative to other radios can mean the radio is underutilized or overutilized relative to the other radios. (However, if the clients are VoIP phones, a relatively high number of clients<br>does not necessarily mean overutilization since voice clients consume less bandwidth on average than data clients.) |
| MIC Error Ct | Number of times the radio received a TKIP-encrypted frame with an invalid MIC.<br><br>Normally, the value of this counter should always be 0. If the value is not 0, check the system log for MIC error messages and contact D-Link Technical Support. |
| TKIP Decrypt Err | Number of times a decryption error occurred with a packet encrypted with TKIP.<br>(See the description for CCMP Pkt Decrypt Err.) |
| CCMP Pkt Replays | Number of CCMP packets that were resent to the AP by a client.<br>(See the description for TKIP Pkt Replays.) |
| RadioResets | Number of times the radio has been reset. Generally, a reset occurs as a result of RF noise. It is normal for this counter to increment a few times per day. |
| Transmit Retries | Number of times the radio retransmitted a unicast packet because it was not acknowledged. The AP uses this counter to adjust the transmit data rate for a client, in order to minimize retries.<br><br>The ratio of transmit retries to transmitted packets (TxUniPkt) indicates the overall transmit quality. A ratio of about 1 retry to 10 transmitted packets indicates good transmit quality. A ratio of 3 or more to 10 indicates poor transmit quality.<br><br>**Note:** This counter includes unacknowledged probes. Some clients do not respond to probes, which can make this counter artificially high. |
| Noise Floor | Received signal strength at which the AP can no longer distinguish 802.11 packets from ambient RF noise. A value around -90 or higher is good for an 802.11b/g radio. A value around -80 or higher is good for an 802.11a radio. Values near 0 can indicate RF interference. |
| 802.3 Packet Rx Ct | Number of raw 802.3 packets received by the radio. These are LocalTalk (AppleTalk) frames. This counter increments only if LocalTalk traffic is present. |

The counters above are global for all data rates. The counters below are for individual data rates.

**Note:** If counters for lower data rates are incrementing but counters for higher data rates are not incrementing, this can indicate poor throughput. The poor throughput can be caused by interference. If the cause is not interference or the interference cannot be eliminated, you might need to relocate the AP in order to use the higher data rates and therefore improve throughput.


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| TxUniPkt | Number of unicast packets transmitted by the radio. |
| TxMultiPkt | Number of multicast packets transmitted by the radio. |
| TxUniByte | Number of unicast bytes transmitted by the radio. |
| TxMultiByte | Number of multicast bytes transmitted by the radio. |
| RxPkt | Number of packets received by the radio. |
| RxByte | Number of bytes received by the radio. |
| UndcrptPkt | Number of undecryptable packets received by the radio. It is normal for this counter to increment even in stable networks and does not necessarily indicate an attack. For example, a client might be sending incorrect key information. However, if the counter increments rapidly, there might be a problem in the network. |
| UndcrptByte | Number of undecryptable bytes received by the radio. (See the description for UndcrptPkt.) |
| PhyError | Number of packets that could not be decoded by the AP. This condition can have any of the following causes:<br><br>• Collision of an 802.11 packet.<br>• Packet whose source is too far away, thus rendering the packet unintelligible by the time it reaches the AP.<br>• Interference caused by an 802.11b/g phone or other source.<br><br>It is normal for this counter to be about 10 percent of the total RxByte count. It is also normal for higher data rates to have higher Phy error counts than lower data rates. |


Download from Www.Somanuals.com. All Manuals Search And Download.

# show {ap | dap} qos-stats

Displays statistics for DWL-8220AP forwarding queues.

**Syntax: show dap qos-stats [*dap-num*] [clear]**

**Syntax: show ap qos-stats [*port-list*] [clear]**

| | |
|---|---|
| *dap-num* | Number of a Distributed AP for which to display QoS statistics counters. |
| *port-list* | List of ports connected to the DWL-8220AP access point(s) for which to display QoS statistics counters. |
| **clear** | Clears the counters after displaying their current values. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** Repeating this command with the clear option at regular intervals allows you to monitor transmission and drop rates.

**Examples:** The following command shows statistics for the AP forwarding queues on a Distributed AP:

```
DWS-1008# set service-profile sp2 wpa-ie enable
CoS    Queue                    Tx          TxDrop
=========================================
          DAP: 4 radio: 1
 1,2   Background               0               0
 0,3   BestEffort           15327             278
 4,5   Video                    0               0
 6,7   Voice                                    0
          DAP: 4 radio: 2
 1,2   Background               0               0
 0,3   BestEffort               0               0
 4,5   Video                    0               0
 6,7   Voice                    0               0
```

The following Table describes the fields in this display:


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| CoS | CoS value associated with the forwarding queues. |
| Queue | Forwarding queue. |
| DAP or Port | Distributed AP number or DWL-8220AP port number. |
| radio | Radio number. |
| Tx | Number of packets transmitted to the air from the queue. |
| TxDrop | Number of packets dropped from the queue instead of being transmitted.<br><br>Some packet drops are normal, especially if the RF environment is noisy. Also, it is normal for a mildly congested radio to drop low-priority packets proportionally more often than high-priority packets. However, continuous packet drops from the Voice queue can indicate over-subscription or excessive interference in the RF environment. |

# show {ap | dap} etherstats

Displays Ethernet statistics for an DWL-8220AP's Ethernet ports.

**Syntax: show {ap | dap} etherstats [***port-list* **|** *dap-num***]**

*port-list* List of DWS-1008 ports directly connected to the DWL-8220AP access point(s) for which to display counters.

*dap-num* Number of a Distributed AP for which to display counters.

**Defaults:** None.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command displays Ethernet statistics for the Ethernet ports on Distributed AP 1:

```
DWS-1008# show dap etherstats 1
DAP: 1                          ether: 1
================================
RxUnicast:          75432       TxGoodFrames:       55210
RxMulticast:        18789       TxSingleColl:          32
RxBroadcast:            8       TxLateColl:             0
RxGoodFrames:       94229       TxMaxColl:              0
RxAlignErrs:            0       TxMultiColl:           47
RxShortFrames:          0       TxUnderruns:            0
RxCrcErrors:            0       TxCarrierLoss:          0
RxOverruns:             0       TxDeferred:           150
RxDiscards:             0

DAP: 1 ether: 2
================================
RxUnicast:          64379       TxGoodFrames:       60621
RxMulticast:        21798       TxSingleColl:          32
RxBroadcast:           11       TxLateColl:             0
RxGoodFrames:       86188       TxMaxColl:              0
RxAlignErrs:            0       TxMultiColl:           12
RxShortFrames:          0       TxUnderruns:            0
RxCrcErrors:            0       TxCarrierLoss:          0
RxOverruns:             0       TxDeferred:           111
RxDiscards:             0
```

The following Table describes the fields in this display:

| Field | Description |
|---|---|
| RxUnicast | Number of unicast frames received. |
| RxMulticast | Number of multicast frames received. |
| RxBroadcast | Number of broadcast frames received. |
| RxGoodFrames | Number of frames received properly from the link. |
| RxAlignErrs | Number of received frames that were both misaligned and contained a CRC error. |
| RxShortFrames | Number of received frames that were shorter than the minimum frame length. |
| RxCrcErrors | Number of received frames that were discarded due to CRC errors. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| RxOverruns | Number of frames known to be lost due to a temporary lack of hardware resources. |
| RxDiscards | Number of frames known to be lost due to a temporary lack of software resources. |
| TxGoodFrames | Number of frames transmitted properly on the link. |
| TxSingleColl | Number of transmitted frames that encountered a single collision. |
| TxLateColl | Number of frames that were not transmitted because they encountered a collision outside the normal collision window. |
| TxMaxColl | Number of frames that were not transmitted because they encountered the maximum allowed number of collisions. Typically, this occurs only during periods of heavy traffic on the network. |
| TxMultiColl | Number of transmitted frames that encountered more than one collision. |
| TxUnderruns | Number of frames that were not transmitted or retransmitted due to temporary lack of hardware resources. |
| TxCarrierLoss | Number of frames transmitted despite the detection of a deassertion of CRS during the transmission. |
| TxDeferred | Number of frames deferred before transmission due to activity on the link. |

# show {ap | dap} group

Displays configuration information and load-balancing status for DWL-8220AP access point groups.

**Syntax: show {ap | dap} group [***name***]**

*name* Name of an AP group or Distributed AP group.

**Defaults:** None.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command displays information for DWL-8220AP access point group *loadbalance1*:

DWS-1008# **set service-profile sp2 wpa-ie enable**

| Load Balance Grp | Port | Clients | Status | Refused |
|---|---|---|---|---|
| loadbalance1 | 1 | 1 | Accepting | 0 |
| loadbalance2 | 7 | 6 | Refusing | 2 |

The following Table describes the fields in this display:

| Field | Description |
|---|---|
| Load Balance Grp | Name of the DWL-8220AP access point group. |
| Port | DWS-1008 port number. |
| Clients | Number of active client sessions on the DWL-8220AP access point. |
| Status | Association status of the DWL-8220AP access point:<br>• Accepting—The access point is accepting new associations.<br>• Refusing—The access point is refusing new associations. |
| Refused | Number of association requests refused by the DWL-8220AP access point due to load balancing. MSS resets this counter to 0 when the DWS-1008 is restarted, MSS is reloaded, or the access point is removed from the group. |


Download from Www.Somanuals.com. All Manuals Search And Download.

# show {ap | dap} status

Displays DWL-8220AP access point and radio status information.

**Syntax: show ap status [terse] | [*port-list* | all [radio {1 | 2}]]**

**Syntax: show dap status [terse] | [*dap-num* | all [radio {1 | 2}]]**

| | |
|---|---|
| **terse** | Displays a brief line of essential status information for each AP. |
| *port-list* | List of ports connected to the DWL-8220AP access point(s) for which to display status. |
| *dap-num* | Number of a Distributed AP for which to display status. |
| **all** | Shows status information for all directly attached DWL-8220AP access points and all Distributed AP access points configured on the switch. |
| **radio1** | Shows status information for radio 1. |
| **radio2** | Shows status information for radio 2. (This option does not apply to single-radio models.) |

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command displays the status of a Distributed AP access point:

```
DWS-1008# show dap status 1
Dap: 1, IP-addr: 10.2.30.5 (vlan 'vlan-corp'), AP model: DWL-8220AP,
manufacturer: D-Link, name: DAP01
fingerprint: b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
==================================================
State: operational (not encrypted) CPU info: IBM:PPC speed=266666664 Hz
version=405GPrid=0x29c15335347f1919 ram=33554432 s/n=0333703027 hw_rev=A3

Uptime: 18 hours, 36 minutes, 27 seconds
Radio 1 type: 802.11g, state: configure succeed [Enabled] (802.11b protect)
 operational channel: 1 operational power: 14 base mac: 00:0b:0e:00:d2:c0
bssid1: 00:0b:0e:00:d2:c0, ssid: public bssid2: 00:0b:0e:00:d2:c2, ssid: employee-net
bssid3: 00:0b:0e:00:d2:c4, ssid: mycorp-tkip

Radio 2 type: 802.11a, state: configure succeed [Enabled] operational channel: 64
operational power: 14 base mac: 00:0b:0e:00:d2:c1 bssid1: 00:0b:0e:00:d2:c1, ssid:
public bssid2: 00:0b:0e:00:d2:c3, ssid: employee-net bssid3: 00:0b:0e:00:d2:
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The following command displays the status of a Distributed AP access point:

```
DWS-1008# show ap status 1
Port: 1, AP model: DWL-8220AP, manufacturer D-Link, name: AP01
================================================
State: operational CPU info: IBM:PPC speed=266666664 Hz version=405GPr
id=0x28b08a1e047f1d0f ram=33554432 s/n=0333000288 hw_rev=A3

Uptime: 3 hours, 44 minutes, 28 seconds
Radio 1 type: 802.11g, state: configure succeed [Enabled] (802.11b protect)
operational channel: 1 operational power: 15 base mac: 00:0b:0e:00:d1:00
bssid1: 00:0b:0e:00:d1:00, ssid: public bssid2: 00:0b:0e:00:d1:02, ssid: empl-net
bssid3: 00:0b:0e:00:d1:04, ssid: mycorp-tkip

Radio 2 type: 802.11a, state: configure succeed [Enabled]
operational channel: 48 operational power: 11 base mac: 00:0b:0e:00:d1:01
bssid1: 00:0b:0e:00:d1:01, ssid: public bssid2: 00:0b:0e:00:d1:03, ssid: empl-net
bssid3: 00:0b:0e:00:d1:05, ssid: mycorp-tkip
```

The following command uses the terse option to display brief information for Distributed APs:

```
DWS-1008# show dap status terse
Total number of entries: 4
Operational: 1, Image Downloading: 0, Unknown: 3, Other: 0
Flags: o = operational, b = booting, d = image downloading
   c = configuring, f = configuration failed a = auto DAP,
   i = insecure
```

| Port | Flg | IP Address | Model | Mac Address | Radio 1 | Radio 2 | Uptime |
|---|---|---|---|---|---|---|---|
| 3 | --- | | DWL-8220AP | | D ?/? | D ?/? | 0d 0h 0m 0s |
| Dap 1 | --- | | DWL-8220AP | | D ?/? | D ?/? | 0d 0h 0m 0s |
| Dap 2 | --- | | DWL-8220AP | | D ?/? | D ?/? | 0d 0h 0m 0s |
| Dap100 | oa- | 10.8.255.11 | DWL-8220AP | 00:0b:0e:da:da:82 | E 1/17 | E36/11 | 0d 0h 0m17s |

The following table describe the fields in these displays:


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| DAP | Connection ID for the Distributed AP.<br><br>Note: This field is applicable only if the AP is configured on the DWS-1008 as a Distributed AP. |
| Port | DWS-1008 port number.<br><br>**Note:** This field is applicable only if the AP is directly connected to the DWS-1008 and the DWS-1008's port is configured as an AP access port. |
| IP-addr | IP address of the AP. The address is assigned to the AP by a DHCP server.<br><br>**Note:** This field is applicable only if the AP is configured on the DWL-8220AP as a Distributed AP. |
| AP model | Access point model number. |
| manufacturer | Company that made the access point. |
| fingerprint | Hexadecimal fingerprint of the AP's public encryption key.<br><br>**Note:** This field is displayed only for Distributed APs. |
| name | AP access point name. |
| Link | Status of this link with the DWL-8220AP access point and the DWL-8220AP port at the other end of the link. The status can be up or down. |
| AP port | AP port number connected to this DWS-1008 port. |
| State | State of the AP:<br>• init—The AP has been recognized by the DWS-1008 but has not yet begun booting.<br>• booting—The AP has asked the DWS-1008 for a boot image.<br>• image downloading—The AP is receiving a boot image from the DWS-1008.<br>• image downloaded—The AP has received a boot image from the DWS-1008 and is booting.<br>• configuring—The AP has booted and is ready to receive or is already receiving configuration parameters from the DWS-1008.<br>• operational—The AP has received configuration parameters for one or more radios and is ready to accept client connections.<br>• configure failure—One or more of the radio parameters received from the DWL-1008 is invalid.<br><br>For Distributed APs, this field also indicates whether the AP's management traffic with the DWS-1008 is encrypted, and whether the AP's fingerprint has been verified on the DWS-1008:<br>• not encrypted—The management session is not encrypted.<br>• encrypted but fingerprint not verified—The AP's management traffic is encrypted, but the AP's fingerprint has not been verified in MSS.<br>• encrypted and verified—The AP's management traffic is encrypted and the AP's fingerprint has been verified in MSS. |
| CPU info | Specifications and identification of the CPU. |
| Uptime | Amount of time since the AP booted using this link. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| Radio 1 type<br>Radio 2 type | 802.11 type and configuration state of the radio.<br>• The configure succeed state indicates that the AP has received configuration parameters for the radio and the radio is ready to accept client connections.<br>• 802.11b protect indicates that the 802.11b/g radio is sending messages to 802.11b devices, while sending 802.11g traffic at higher data rates, to inform the 802.11b devices about the 802.11g traffic and reserve bandwidth for the traffic.<br><br>Protection mode remains in effect until 60 seconds after the last 802.11b traffic is detected by the 802.11b/g radio.<br>• Sweep Mode indicates that a disabled radio is nonetheless participating in rogue detection scans. Even though this message appears only for disabled radios, all radios, enabled or disabled, participate in rogue detection.<br>• Countermeasures Enabled indicates that the radio is sending countermeasures packets to combat a rogue.<br>• Radar Scan indicates that the radio is performing the initial channel availability check for Dynamic Frequency Selection (DFS). This state lasts during the first 60 seconds an 802.11a radio is on a new channel, during which time the radio does not transmit. If the radio does not detect any radar on the channel, the radio starts using the channel for data. If the radio does detect radar, the flag changes to Radar Detected.<br>• Radar Detected indicates that DFS has detected radar on the channel. When this occurs, the AP stops transmitting on the channel for 30 minutes.<br><br>If RF Auto-Tuning is enabled for channel assignment, the radio selects another channel and performs the initial channel availability check on the new channel, during which time the flag changes back to Radar Scan.<br><br>**Note:** Radar Scan and Radar Detected apply only to 802.11a radios, for country codes that use DFS.<br>• The following information appears for external antennas:<br>• External antenna detected, configured as antenna-model—Indicates that an external antenna has been detected, and lists the antenna model configured on the radio. (MSSdoes not detect the specific model. |
| operational channel | The channel on which the radio is currently operating.<br><br>**Note:** If the channel number is followed by (Auto), the value was set by RF Auto-Tuning. |
| operational power | The power level at which the radio is currently operating.<br><br>**Note:** If the power setting is followed by (Auto), the value was set by RF Auto-Tuning. |
| base mac | Base MAC address of the radio. |
| bssid, ssid | SSIDs configured on the radio and their BSSIDs. |
| RFID Reports | Status of AeroScout asset tag support.<br>• Active—The AeroScout Engine has enabled the tag report mode on the AP.<br>• Inactive—The AeroScout Engine has not enabled, or has disabled, the tag report mode on the AP.<br><br>**Note:** This field is displayed only if the rfid-mode option is enabled on the radio profile that manages the radio. |


Download from Www.Somanuals.com. All Manuals Search And Download.

### Output for show ap status terse and show dap status terse

| Field | Description |
|---|---|
| Port | DWS-1008AP port number connected to the AP. |
| Flg | Operational status flags for the AP.<br><br>For flag definitions, see the key in the command output. |
| IP Address | IP address of the AP. The address is assigned to the AP by a DHCP server.<br><br>**Note:** This field is applicable only if the AP is configured on the DWS-1008 as a Distributed AP. |
| Model | AP model number. |
| MAC Address | MAC address of the AP. |
| Radio1 | State, channel, and power information for radio 1:<br>• The state can be D (disabled) or E (enabled).<br>• The channel and power settings are shown as channel/power. |
| Radio2 | State, channel, and power information for radio 2. |
| Uptime | Amount of time since the AP booted using this link. |

## show auto-tune attributes

Displays the current values of the RF attributes RF Auto-Tuning uses to decide whether to change channel or power settings.

**Syntax show auto-tune attributes [ap** *mp-num* **[radio {1 | 2| all}]]**

**Syntax show auto-tune attributes [dap** *dap-num* **[radio {1 | 2| all}]]**

*mp-num* AP port connected to the AP access point for which to display RF attributes.

*dap-num* Number of a Distributed AP for which to display RF attributes.

**radio1** Shows RF attribute information for radio 1.

**radio2** Shows RF attribute information for radio 2.

**radio all** Shows RF attribute information for both radios.

**Defaults** None.

**Access** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command displays RF attribute information for radio 1 on the directly connected DWL-8220AP access point on port 2:

```
DWS-1008# show auto-tune attributes ap 2 radio 1
Auto-tune attributes for port 2 radio 1:
Noise:          -92          Packet Retransmission Count:      0
Utilization:    0            Phy Errors Count:                 0
CRC Errors count:   122
```

The following table describes the fields in the display:

| Field | Description |
|---|---|
| Noise | Noise threshold on the active channel. RF Auto-Tuning prefers channels with low noise levels over channels with higher noise levels. |
| Utilization | Number of multicast packets per second that a radio can send on a channel while continuously sending fixed size frames over a period of time. The number of packets that are successfully transmitted indicates how busy the channel is. |
| CRC Errors count | Number of frames received by the radio on that active channel that had CRC errors. A high CRC error count can indicate a hidden node or co-channel interference. |
| Packet Retransmission Count | Number of retransmitted packets sent from the client to the radio on the active channel. Retransmissions can indicate that the client is not receiving ACKs from the AP radio. |
| Phy Errors Count | Number of frames received by the AP radio that had physical layer errors on the active channel. Phy errors can indicate interference from a non-802.11 device. |

**See Also:**

- set {ap | dap} radio auto-tune max-power
- set radio-profile auto-tune channel-config
- set radio-profile auto-tune channel-holddown
- set radio-profile auto-tune channel-interval
- set radio-profile auto-tune power-config
- set radio-profile auto-tune power-interval
- show auto-tune neighbors
- show radio-profile


Download from Www.Somanuals.com. All Manuals Search And Download.

# show auto-tune neighbors

Displays the other D-Link access point and third-party 802.11 access points that a D-Link access point can hear.

**Syntax: show auto-tune neighbors [ap** *mp-num* **[radio {1 | 2| all}]]**

**Syntax: show auto-tune neighbors [dap dap-num [radio {1 | 2| all}]]**

*mp-num* AP port connected to the AP access point for which to display neighbors.

*dap-num* Number of a Distributed AP for which to display neighbors.

**radio1** Shows neighbor information for radio 1.

**radio2** Shows neighbor information for radio 2.

**radio all** Shows neighbor information for both radios.

**Defaults:** None.

**Access:** Enabled.

**Usage:** For simplicity, this command displays a single entry for each D-Link radio, even if the radio is supporting multiple BSSIDs. However, BSSIDs for third-party 802.11 radios are listed separately, even if a radio is supporting more than one BSSID.

Information is displayed for a radio if the radio sends beacon frames or responds to probe requests. Even if a radio's SSIDs are unadvertised, D-Link radios detect the empty beacon frames (beacon frames without SSIDs) sent by the radio, and include the radio in the neighbor list.

**Examples:** The following command displays neighbor information for radio 1 on the directly connected AP access point on port 2:

```
DWS-1008# show auto-tune neighbors ap 2 radio 1
Total number of entries for port 2 radio 1: 5
Channel   Neighbor  BSS/MAC   RSSI
-----------  --------------------------  ------
        1   00:0b:85:06:e3:60       -46
        1   00:0b:0e:00:0a:80       -78
        1   00:0b:0e:00:d2:c0       -74
        1   00:0b:85:06:dd:00       -50
        1   00:0b:0e:00:05:c1       -72
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The following table describes the fields in the display:

| Field | Description |
|---|---|
| Channel | Channel on which the BSSID is detected. |
| Neighbor BSS/MAC | BSSID detected by the radio. |
| RSSI | Received signal strength indication (RSSI), in decibels referred to 1 milliwatt (dBm). A higher value indicates a stronger signal. |

**See Also:**
- set {ap | dap} radio auto-tune max-power
- set radio-profile auto-tune channel-config
- set radio-profile auto-tune channel-holddown
- set radio-profile auto-tune channel-interval
- set radio-profile auto-tune power-config
- set radio-profile auto-tune power-interval
- show auto-tune attributes
- show radio-profile

# show dap boot-configuration

Displays information about the static IP address configuration (if any) on a Distributed AP.

**Syntax: show dap boot-configuration** *dap-num*

*dap-num* Number of a Distributed AP for which to display static IP configuration information.

**Defaults:** None.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command displays static IP configuration information for Distributed AP 1:

```
DWS-1008# show dap boot-configuration 1
Static Boot Configuration
DAP: 1

IP Address:   Disabled
VLAN Tag:     Disabled
Switch:       Disabled

IP Address:
Netmask:
Gateway:
VLAN Tag:
Switch IP:
Switch Name:
DNS IP:
```

The following table describes the fields in the display:

| Field | Description |
|---|---|
| DAP | Distributed AP number. |
| IP Address | Whether static IP address assignment is enabled for this Distributed AP. |
| VLAN Tag | Whether the Distributed AP is configured to use a VLAN tag. |
| Switch | Whether the Distributed AP is configured to use a manually specified DWS-1008 as its boot device. |
| IP Address | The static IP address assigned to this Distributed AP. |
| Netmask | The subnet mask assigned to this Distributed AP. |
| Gateway | The IP address of the default gateway assigned to this Distributed AP. |
| Vlan Tag | The VLAN tag that the Distributed AP is configured to use (if any). |
| Switch IP | The IP address of the DWS-1008 that this Distributed AP is configured to use as its boot device (if any). |
| Switch Name | The name of the DWS-1008 that this Distributed AP is configured to use as its boot device (if any). |
| DNS IP | The IP address of the DNS server that the Distributed AP uses to resolve the name of the DWS-1008 used as its boot device. |


Download from Www.Somanuals.com. All Manuals Search And Download.

# show dap connection

Displays the system IP address of the DWS-1008 that booted a Distributed AP.

**Syntax: show dap connection [***dap-num* **| serial-id** *serial-ID***]**

*dap-num*

Number of a Distributed AP for which to display information about its active connection.

**serial-id**

DWL-8220AP access point serial ID.

**Defaults:** None.

**Access:** Enabled.

**Usage:** The **serial-id** parameter displays the active connection for the specified Distributed AP even if that AP is not configured on this DWS-1008. If you instead use the command with the *dap-num* parameter or without a parameter, connection information is displayed only for Distributed APs that are configured on this DWS-1008.

This command provides information only if the Distributed AP is configured on the switch where you use the command. The switch does not need to be the one that booted the AP, but it must have the AP in its configuration.

If a Distributed AP is configured on this DWS-1008 but does not have an active connection, the command does not display information for the AP. To show connection information for Distributed APs, use the **show dap global** command on one of the switches where the APs are configured.

**Examples:** The following command displays information for all Distributed APs configured on this DWS-1008 that have active connections:

```
DWS-1008# show dap connection
Total number of entries:  2
```

| DAP | Serial Id | DAP IP Address | DWS-1008 IP Address |
|---|---|---|---|
| 2 | 112233 | 10.10.2.27 | 10.3.8.111 |
| 4 | 0333000298 | 10.10.3.34 | 10.3.8.111 |


Download from Www.Somanuals.com. All Manuals Search And Download.

The following command displays information for all Distributed APs configured on this DWS-1008 that have active connections:

```
DWS-1008# show dap connection
Total number of entries:  1
```

| DAP | Serial Id | DAP IP Address | DWS-1008 IP Address |
|---|---|---|---|
| 7 | 223344 | 10.10.4.88 | 10.9.9.11 |

The following table describes the fields in the display:

| Field | Description |
|---|---|
| DAP | Connection ID you assigned to the Distributed AP.<br><br>If the connection is configured on another DWS-1008, this field contains a hyphen ( - ). |
| Serial Id | Serial ID of the Distributed AP. |
| DAP IP Address | IP address assigned by DHCP to the Distributed AP. |
| DWS-1008 IP Address | System IP address of the DWS-1008 on which the AP has an active connection. This is the switch that the AP used for booting and configuration and is using for data transfer. |

# show dap global

Displays connection information for Distributed APs configured on an DWS-1008.

**Syntax: show dap global [***dap-num* **| serial-id** *serial-ID***]**

*dap-num* Number of a Distributed AP for which to display configuration settings.

**serial-id** DWL-8220AP access point serial ID.

**Defaults:** None.

**Access:** Enabled.

**Usage:** Connections are shown only for the Distributed APs that are configured on the DWS-1008 from which you enter the command.


Download from Www.Somanuals.com. All Manuals Search And Download.

To show information only for Distributed APs that have active connections, use the **show dap connection** command.

**Examples:** To show information only for Distributed APs that have active connections, use the show dap connection command.

DWS-1008# **show dap global**
Total number of entries: 8

| DAP | Serial Id | DWS-1008 IP Address | Bias |
|---|---|---|---|
| 1 | 11223344 | 10.8.8.111 | HIGH |
| - | 11223344 | 10.4.3.2 | LOW |
| 2 | 332211 | 10.3.8.111 | LOW |
| - | 332211 | 10.4.3.2 | HIGH |
| 7 | 0332210018 | 10.3.8.111 | HIGH |
| - | 0332210018 | 10.4.3.2 | LOW |
| 8 | 0321250012 | 10.3.8.111 | LOW |
| - | 0321250012 | 10.4.3.2 | HIGH |

The following table describes the fields in the display:

| Field | Description |
|---|---|
| DAP | Connection ID you assigned to the Distributed AP.<br><br>**Note:** DAP numbers are listed only for Distributed APs configured on this DWS-1008. If the field contains a hyphen ( - ), the Distributed AP configuration displayed in the row of output is on another DWS-1008. |
| Serial Id | Serial ID of the Distributed AP. |
| DAP IP Address | System IP address of the DWS-1008 on which the Distributed AP is configured. A separate row of output is displayed for each DWS-1008 on which the Distributed AP is configured. |
| Bias | Bias of the DWS-1008 for the Distributed AP:<br>• High<br>• Low |


Download from Www.Somanuals.com. All Manuals Search And Download.

# show dap unconfigured

Displays Distributed APs that are physically connected to the network but that are not configured on any DWS-1008s.

**Syntax: show dap unconfigured**

**Defaults:** None.

**Access:** Enabled.

**Usage:** This command also displays an AP that is directly connected to an DWS-1008, if the switch port to which the AP is connected is configured as a network port instead of an AP access port, and if the network port is a member of a VLAN.

Entries in the command output's table age out after two minutes.

**Examples:** The following command displays information for two Distributed APs that are not configured:

```
DWS-1008# show dap unconfigured
Total number of entries:  2
```

| Serial Id | Model | IP Address | Port | Vlan |
|---|---|---|---|---|
| 0333001287 | DWL-8220AP | 10.3.8.54 | 5 | default |
| 0333001285 | DWL-8220AP | 10.3.8.57 | 7 | vlan-eng |

The following table describes the fields in the display:

| Field | Description |
|---|---|
| Serial Id | Serial ID of the Distributed AP. |
| Model | AP model number. |
| IP Address | IP address of the AP. This is the address that the AP receives from a DHCP server. The AP uses this address to send a Find DWS message to request configuration information from DWL-1008.<br><br>However, the AP cannot use the address to establish a connection unless the AP first receives a configuration from an DWS-1008. |
| Port | Port number on which this DWS-1008 received the AP's Find DWS message. |
| VLAN | VLAN on which this DWS-1008 received the AP's Find DWS message. |


Download from Www.Somanuals.com. All Manuals Search And Download.

# show radio-profile

Displays radio profile information.

**Syntax: show radio-profile {***name* **| ?}**

*name* Displays information about the named radio profile.

**?** Displays a list of radio profiles.

**Defaults:** None.

**Access:** Enabled.

**Usage:** MSS contains a default radio profile. D-Link recommends that you do not change this profile but instead keep the profile for reference.

**Examples:** The following command shows radio profile information for the default radio profile:

```
DWS-1008# show radio-profile default
Beacon Interval:          100          DTIM Interval:            1
Max Tx Lifetime:          2000         Max Rx Lifetime:          2000
RTS Threshold:            2346         Frag Threshold:           2346
Long Preamble:            no           Tune Channel:             yes
Tune Power:               no           Tune Channel Interval:    3600
Tune Power Interval:      600          Power ramp interval:      60
Channel Holddown:         300          Countermeasures:          none
Active-Scan:              yes          RFID enabled:             no
WMM Powersave:            no           QoS Mode:                 wmm

No service profiles configured.
```

The following table describes the fields in the display:

| Field | Description |
|---|---|
| Beacon Interval | Rate (in milliseconds) at which each AP radio in the profile advertises the beaconed SSID. |
| DTIM Interval | Number of times after every beacon that each AP radio in the radio profile sends a delivery traffic indication map (DTIM). |
| Max Tx Lifetime | Number of milliseconds that a frame received by a radio in the radio profile can remain in buffer memory. |
| Max Rx Lifetime | Number of milliseconds that a frame scheduled to be transmitted by a radio in the radio profile can remain in buffer memory. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| RTS Threshold | Minimum length (in bytes) a frame can be for a radio in the radio profile to use the RTS/CTS method to send the frame. The RTS/CTS method clears the air of other traffic to avoid corruption of the frame due to a collision with another frame. |
| Frag Threshold | Maximum length (in bytes) a frame is allowed to be without being fragmented into multiple frames before transmission by a radio in the radio profile. |
| Long Preamble | Indicates whether an 802.11b radio that uses this radio profile advertises support for frames with long preambles only:<br><br>• YES—Advertises support for long preambles only.<br>• NO—Advertises support for long and short preambles. |
| Tune Channel | Indicates whether RF Auto-Tuning is enabled for dynamically setting and tuning channels. |
| Tune Power | Indicates whether RF Auto-Tuning is enabled for dynamically setting and tuning power levels. |
| Tune Channel Interval | Interval, in seconds, at which RF Auto-Tuning decides whether to change the channels on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed<br>during the previous interval, and changes radio channels if needed. |
| Tune Power Interval | Interval, in seconds, at which RF Auto-Tuning decides whether to change the power level on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio power levels if needed. |
| Power ramp interval | Number of seconds a radio waits before increasing or decreasing its power by 1 dBm in response to a power change from RF Auto-Tuning. After each power ramp interval, the radio increases or decreases the power by another 1 dB until the radio reaches the power level selected by RF Auto-Tuning. |
| Channel Holddown | Minimum number of seconds a radio in a radio profile must remain at its current channel assignment before RF Auto-Tuning can change the channel. |
| Countermeasures | Indicates whether countermeasures are enabled. |
| Active-Scan | Indicates whether the active-scan mode of RF detection is enabled. |
| RFID enabled | Indicates whether AeroScout tag support is enabled. |
| WMM Powersave | Indicates whether U-APSD support is enabled. |
| QoS Mode | Indicates the Quality-of-Service setting for AP radio forwarding queues:<br>• wmm—AP forwarding queues provide standard priority handling for WMM devices.<br>• svp—AP forwarding queues are optimized for SpectraLink Voice Priority (SVP). |
| Service profiles | Service profiles mapped to this radio profile. Each service profile contains an SSID and encryption information for that SSID. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**See Also:**

- set radio-profile active-scan
- set radio-profile auto-tune channel-config
- set radio-profile auto-tune channel-holddown
- set radio-profile auto-tune channel-interval
- set radio-profile auto-tune channel-lockdown
- set radio-profile auto-tune power-config
- set radio-profile auto-tune power-interval
- set radio-profile auto-tune power-lockdown
- set radio-profile auto-tune power-ramp-interval
- set radio-profile beacon-interval
- set radio-profile countermeasures
- set radio-profile dtim-interval
- set radio-profile frag-threshold
- set radio-profile max-rx-lifetime
- set radio-profile max-tx-lifetime
- set radio-profile mode
- set radio-profile preamble-length
- set radio-profile qos-mode
- set radio-profile rfid-mode
- set radio-profile rts-threshold
- set radio-profile service-profile
- set radio-profile wmm-powersave


Download from Www.Somanuals.com. All Manuals Search And Download.

# show service-profile

Displays service profile information.

**Syntax show service-profile {*name* | ?}**

*name* Displays information about the named service profile.

**?** Displays a list of service profiles.

**Defaults** None.

**Access** Enabled.

**Examples** The following command displays information for service profile sp1:

```
DWS-1008# show service-profile sp1
ssid-name:                  corp2                ssid-type:                  crypto
Beacon:                     yes                  Proxy ARP:                  no
DHCP restrict:              no                   No broadcast:               no
Short retry limit:          5                    Long retry limit:           5
Auth fallthru:              none                 Sygate On-Demand (SODA):    no
Enforce SODA checks:        yes                  SODA remediation            ACL:
Custom success web-page:                         Custom failure web-page:
Custom logout web-page:                          Custom agent-directory:
Static COS:                 no                   COS:                        0
CAC mode:                   none                 CAC sessions:               14
User idle timeout:          180                  Idle client probing:        yes
Keep initial vlan:          no                   Web Portal Session Timeout: 5
Web Portal ACL:
WEP Key 1 value:            <none>               WEP Key 2 value:            <none>
WEP Key 3 value:            <none>               WEP Key 4 value:            <none>
WEP Unicast Index:          1                    WEP Multicast Index:        1
Shared Key Auth:             NO
WPA enabled:
        ciphers: cipher-tkip
        authentication: 802.1X
        TKIP countermeasures time: 60000ms
vlan-name = orange
session-timeout = 300
service-type = 2
11a beacon rate:            6.0                  multicast rate:             AUTO
11a mandatory rate: 6.0,12.0,24.0       standard rates: 9.0,18.0,36.0,48.0,54.0
11b beacon rate:             2.0                 multicast rate:             AUTO
11b mandatory rate: 1.0,2.0             standard rates: 5.5,11.0
11g beacon rate: 2.0                             multicast rate:             AUTO
11g mandatory rate: 1.0,2.0,5.5,11.0 standard rates: 6.0,9.0,12.0,18.0,24.0, 36.0,48.0,54.0
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The following table describes the fields in the display:

| Field | Description |
|---|---|
| ssid-name | Service set identifier (SSID) managed by this service profile. |
| ssid-type | SSID type:<br>• crypto—Wireless traffic for the SSID is encrypted.<br>• clear—Wireless traffic for the SSID is unencrypted. |
| Beacon | Indicates whether the radio sends beacons, to advertise the SSID:<br>• no<br>• yes |
| Proxy ARP | Indicates whether proxy ARP is enabled. When this feature is enabled, MSS answers ARP requests on behalf of wireless clients. |
| DHCP restrict | Indicates whether DHCP Restrict is enabled. When this feature is enabled, MSS allows only DHCP traffic for a new client until the client has successfully completed authentication and authorization. |
| No broadcast | Indicates whether broadcast restriction is enabled. When this feature is enabled, MSS sends ARP requests and DHCP Offers and Acks as unicasts to their target clients instead of forwarding them as broadcasts. |
| Short retry limit | Number of times a radio serving the service-profile's SSID can send a short unicast frame without receiving an acknowledgment. |
| Long retry limit | Number of times a radio serving the service-profile's SSID can send a long unicast frame without receiving an acknowledgment. A long unicast frame is a frame that is *equal* to or *longer* than the RTS threshold. |
| Auth fallthru | Secondary (fallthru) encryption type when a user tries to authenticate but the DWL-1008 switch managing the radio does not have an authentication rule with a userglob that matches the username.<br><br>• last-resort—Automatically authenticates the user and allows access to the SSID requested by the user, without requiring a username and password.<br>• none—Denies authentication and prohibits the user from accessing the SSID.<br>• web-portal—Redirects the user to a web page for login to the SSID. |
| Sygate On-Demand (SODA) | Whether SODA functionality is enabled for the service profile. When SODA functionality is enabled, connecting clients download SODA agent files, which perform security checks on the client. |
| Enforce SODA checks | Whether a client is allowed access to the network after it has downloaded and run the SODA agent security checks. When SODA functionality is enabled, and the DWS-1008 is configured to enforce SODA checks, then a connecting client must download the SODA agent files and pass the checks in order to gain access to the network. |
| SODA remediation ACL | The name of the ACL to be applied to the client if it fails the SODA agent checks. If no remediation ACL is specified, then a client is disconnected from the network if it fails the SODA agent checks. |
| Custom success web-page | The name of the user-specified page that the client loads upon successful completion of the SODA agent checks. If no page is specified, then the success page is generated dynamically. |
| Custom failure web-page | The name of the user-specified page that the client loads if it fails SODA agent checks. If no page is specified, then the failure page is generated dynamically. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| Custom logout web-page | The name of the user-specified page that the client loads upon logging out of the network, either by closing the SODA virtual desktop, or by requesting the page. If no page is specified, then the client is disconnected without loading a logout page. |
| Custom agent-directory | The name of the directory for SODA agent files on the DWS-1008, if different from the default. By default, SODA agent files are stored in a directory with the same name as the service profile. |
| Static COS | Indicates whether static CoS assignment is enabled. When this feature is enabled, APs assign the CoS value in the COS field to all user traffic forwarded by the AP. |
| COS | CoS value assigned by the AP to all user traffic, if static CoS is enabled. (If static CoS is disabled, WMM or ACLs are used to assign CoS.) |
| CAC mode | Call Admission Control mode:<br>• none—CAC is disabled.<br>• session—CAC is based on the number of active user sessions. If an AP radio reaches the maximum number of active user sessions specified in the CAC session field, the AP radio rejects new connection attempts. |
| CAC sessions | Maximum number of user sessions that can be active on an AP radio at one time, if the CAC mode is session. (If the CAC mode is none, this value is not used.) |
| User idle timeout | Indicates how many seconds a user session can remain idle (indicated by no user traffic and no reply to client keepalive probes) before the session is changed to the Disassociated state. |
| Idle client probing | Indicates whether client keepalive probes are enabled. |
| Keep initial VLAN | Indicates whether the **keep-initial-vlan** option is enabled. |
| Web Portal Session Timeout | When a Web Portal WebAAA session is placed in the Deassociated state, how many seconds the session can remain in that state before being terminated automatically. |
| Web Portal ACL | Name of the ACL used to filter traffic for Web Portal users associated with this service profile's SSID while the users are being authenticated. |
| WEP Key 1 value | State of static WEP key number 1. Radios can use this key to encrypt traffic with static Wired-Equivalent Privacy (WEP):<br>• none—The key is not configured.<br>• preset—The key is configured.<br><br>**Note:** The WEP parameters apply to traffic only on the encrypted SSID. |
| WEP Key 2 value | State of static WEP key number 2:<br>• none—The key is not configured.<br>• preset—The key is configured. |
| WEP Key 3 value | State of static WEP key number 3:<br>• none—The key is not configured.<br>• preset—The key is configured. |
| WEP Key 4 value | State of static WEP key number 4:<br>• none—The key is not configured.<br>• preset—The key is configured. |
| WEP Unicast Index | Index of the static WEP key used to encrypt unicast traffic on an encrypted SSID. |
| WEP Multicast Index | Index of the static WEP key used to encrypt multicast traffic on an encrypted SSID. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| Shared Key Auth | Indicates whether shared-key authentication is enabled. |
| WPA enabled<br>or<br>RSN enabled | Indicates that the Wi-Fi Protected Access (WPA) or Robust Security Network (RSN) information element (IE) is enabled. Additional fields display the settings of other WPA or RSN parameters:<br>• ciphers—Lists the cipher suites advertised by radios in the radio profile mapped to this service profile.<br>• authentication—Lists the authentication methods supported for WPA or RSN clients:<br>• 802.1X—dynamic authentication<br>• PSK—preshared key authentication<br>• TKIP countermeasures time—Indicates the amount of time (in ms) MSS enforces countermeasures following a second message integrity code (MIC) failure within a 60-second period.<br><br>**Note:** These fields are displayed only when the WPA IE or RSN IE is enabled. |
| vlan-name,<br>session-timeout,<br>service-type | These are examples of authorization attributes that are applied by default to a user accessing the SSID managed by this service profile (in addition to any attributes assigned to the user by a RADIUS server or the local database).<br><br>Attributes are listed here only if they have been configured as default attribute settings for the service profile. |
| 11a / 11b / 11g transmit rate fields | Data transmission rate settings for each radio type:<br>• beacon rate—Data rate of beacon frames sent by AP radios.<br>• multicast rate—Data rate of multicast frames sent by AP radios. If the rate is auto, the AP sets the multicast rate to the highest rate that can reach all clients connected to the radio.<br>• mandatory rates—Set of data transmission rates that clients are required to support in order to associate with an SSID on an AP radio. A client must support at least one of the mandatory rates.<br>• standard rates—The set of valid rates that are neither mandatory nor disabled. These rates are supported for data transmission from the AP radios.<br>• disabled rates—Data transmission rates that AP radios will not use to transmit data. (The radios will still accept frames from clients at disabled data rates.) |


Download from Www.Somanuals.com. All Manuals Search And Download.

# STP Commands

Use Spanning Tree Protocol (STP) commands to configure and manage spanning trees on the virtual LANs (VLANs) configured on a switch, to maintain a loop-free network. This chapter presents STP commands alphabetically. Use the following table to locate commands in this chapter based on their use.


| | |
|---|---|
| **STP State** | set spantree on page 492<br>show spantree on page 502<br>show spantree blockedports on page 506 |
| **Bridge Priority** | set spantree priority on page 501 |
| **Port Cost** | set spantree portcost on page 496<br>set spantree portvlancost on page 499<br>show spantree portvlancost on page 508<br>clear spantree portcost on page 488<br>clear spantree portvlancost on page 490 |
| **Port Priority** | set spantree portpri on page 498<br>set spantree portvlanpri on page 500<br>clear spantree portpri on page 489<br>clear spantree portvlanpri on page 491 |
| **Timers** | set spantree fwddelay on page 494<br>set spantree hello on page 495<br>set spantree maxage on page 495 |
| **Fast Convergence** | set spantree portfast on page 498<br>show spantree portfast on page 507<br>set spantree backbonefast on page 493<br>show spantree backbonefast on page 506<br>set spantree uplinkfast on page 502<br>show spantree uplinkfast on page 516 |
| **Statistics** | show spantree statistics on page 509<br>clear spantree statistics on page 492 |




Download from Www.Somanuals.com. All Manuals Search And Download.

# clear spantree portcost

Resets to the default value the cost of a network port or ports on paths to the STP root bridge in all VLANs on a DWS-1008 switch.

**Syntax: clear spantree portcost** *port-list*

| | |
|---|---|
| *port-list* | List of ports. The port cost is reset on the specified ports. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** This command resets the cost in all VLANs. To reset the cost for only specific VLANs, use the **clear spantree portvlancost** command.

**Examples:** The following command resets the STP port cost on ports 5 and 6 to the default value:

```
DWS-1008# clear spantree portcost 5-6
success: change accepted.
```

**See Also:**
- clear spantree portvlancost
- set spantree portcost
- set spantree portvlancost
- show spantree
- show spantree portvlancost

# clear spantree portpri

Resets to the default value the priority of a network port or ports for selection as part of the path to the STP root bridge in all VLANs on a DWS-1008 switch.

**Syntax: clear spantree portpri** *port-list*

| | |
|---|---|
| *port-list* | List of ports. The port priority is reset to 32 (the default) on the specified ports. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** This command resets the priority in all VLANs. To reset the priority for only specific VLANs, use the **clear spantree portvlanpri** command.

**Examples:** The following command resets the STP priority on port 9 to the default:

```
DWS-1008# clear spantree portpri 9
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear spantree portvlancost

Resets to the default value the cost of a network port or ports on paths to the STP root bridge for a specific VLAN on a DWS-1008 switch, or for all VLANs.

**Syntax: clear spantree portvlancost** *port-list* **{all | vlan** *vlan-id***}**

*port-list* List of ports. The port cost is reset on the specified ports.

**all** Resets the cost for all VLANs.

**vlan** *vlan-id* VLAN name or number. MSS resets the cost for only the specified VLAN.

**Defaults:** None.

**Access:** Enabled.

**Usage:** MSS does not change a port's cost for VLANs other than the one(s) you specify.

**Examples:** The following command resets the STP cost for port 12 in VLAN *sunflower*:

```
DWS-1008# clear spantree portvlancost 12 vlan sunflower
success: change accepted.
```

**See Also:**
- clear spantree portcost
- set spantree portcost
- set spantree portvlancost
- show spantree
- show spantree portvlancost

# clear spantree portvlanpri

Resets to the default value the priority of a network port or ports for selection as part of the path to the STP root bridge, on one VLAN or all VLANs.

**Syntax: clear spantree portvlanpri** *port-list* **{all | vlan** *vlan-id***}**

*port-list* List of ports. The port priority is reset to 32 (the default) on the specified ports.

**all** Resets the priority for all VLANs.

**vlan** *vlan-id* VLAN name or number. MSS resets the priority for only the specified VLAN.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** Enabled.

**Usage:** MSS does not change a port's priority for VLANs other than the one(s) you specify.

**Examples:** The following command resets the STP priority for port 5 in VLAN *avocado*:

```
DWS-1008# clear spantree portvlanpri 5 vlan avocado
success: change accepted.
```

**See Also:**
- clear spantree portpri
- set spantree portpri
- set spantree portvlanpri
- show spantree

# clear spantree statistics

Clears STP statistics counters for a network port or ports and resets them to 0.

**Syntax: clear spantree statistics** *port-list* **[vlan** *vlan-id***]**

*port-list* List of ports. Statistics counters are reset on the specified ports.

**vlan** *vlan-id* VLAN name or number. MSS resets statistics counters for only the specified VLAN.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command clears STP statistics counters for ports 1 and 4 through 6 for all VLANs:

```
DWS-1008# clear spantree statistics 1,4-6
success: change accepted.
```

**See Also:**
- show spantree statistics


Download from Www.Somanuals.com. All Manuals Search And Download.

# set spantree

Enables or disables STP on one VLAN or all VLANs configured on a DWS-1008 switch.

**Syntax: set spantree {enable | disable} [{all | vlan** *vlan-id* **| port** *port-list vlan-id***}]**

| | |
|---|---|
| **enable** | Enables STP. |
| **disable** | Disables STP. |
| **all** | Enables or disables STP on all VLANs. |
| **vlan** *vlan-id* | VLAN name or number. MSS enables or disables STP on only the specified VLAN, on all ports within the VLAN. |
| **port** *port-list vlan-id* | Port number or list and the VLAN the ports are in. MSS enables or disables STP on only the specified ports, within the specified VLAN. |

**Defaults:** Disabled.

**Access:** Enabled.

**Examples:** The following command enables STP on all VLANs configured on a switch:

```
DWS-1008# set spantree enable
success: change accepted.
```

The following command disables STP on VLAN *burgundy*:

```
DWS-1008# set spantree disable vlan burgundy
success: change accepted.
```

**See Also:**
• show spantree

# set spantree backbonefast

Enables or disables STP backbone fast convergence on a switch. This feature accelerates a port's recovery following the failure of an indirect link.

**Syntax: set spantree backbonefast {enable | disable}**

| | |
|---|---|
| **enable** | Enables backbone fast convergence. |
| **disable** | Disables backbone fast convergence. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** STP backbone fast path convergence is disabled by default.

**Access:** Enabled.

**Usage:** If you plan to use the backbone fast convergence feature, you must enable it on all the bridges in the spanning tree.

**Examples:** The following command enables backbone fast convergence:

```
DWS-1008# set spantree backbonefast enable
success: change accepted.
```

**See Also:**
• show spantree backbonefast

# set spantree fwddelay

Changes the period of time after a topology change that a switch which is not the root bridge waits to begin forwarding Layer 2 traffic on one or all of its configured VLANs. (The root bridge always forwards traffic.)

**Syntax: set spantree fwddelay delay {all | vlan** *vlan-id***}**

**delay** Delay value. You can specify from 4 through 30 seconds.

**all** Changes the forwarding delay on all VLANs.

**vlan** *vlan-id* VLAN name or number. MSS changes the forwarding delay on only the specified VLAN.

**Defaults:** The default forwarding delay is 15 seconds.

**Access:** Enabled.

**Examples:** The following command changes the forwarding delay on VLAN *pink* to 20 seconds:

```
DWS-1008# set spantree fwddelay 20 vlan pink
success: change accepted.
```

**See Also:**
• show spantree


Download from Www.Somanuals.com. All Manuals Search And Download.

# set spantree hello

Changes the interval between STP hello messages sent by a switch when operating as the root bridge, on one or all of its configured VLANs.

**Syntax: set spantree hello interval {all | vlan** *vlan-id***}**

**interval** Interval value. You can specify from 1 through 10 seconds.

**all** Changes the interval on all VLANs.

**vlan** *vlan-id* VLAN name or number. MSS changes the interval on only the specified VLAN.

**Defaults:** The default hello timer interval is 2 seconds.

**Access:** Enabled.

**Examples:** The following command changes the hello interval for all VLANs to 4 seconds:

```
DWS-1008# set spantree hello 4 all
success: change accepted.
```

**See Also:**
• show spantree

# set spantree maxage

Changes the maximum age for an STP root bridge hello packet that is acceptable to a switch acting as a designated bridge on one or all of its VLANs. After waiting this period of time for a new hello packet, the switch determines that the root bridge is unavailable and issues a topology change message.

**Syntax: set spantree maxage** *aging-time* **{all | vlan** *vlan-id***}**

*aging-time* Maximum age value. You can specify from 6 through 40 seconds.

**all** Changes the maximum age on all VLANs.

**vlan** *vlan-id* VLAN name or number. MSS changes the maximum age on only the specified VLAN.

**Defaults:** The default maximum age for root bridge hello packets is 20 seconds.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command changes the maximum acceptable age for root bridge hello packets on all VLANs to 15 seconds:

```
DWS-1008# set spantree maxage 15 all
success: change accepted.
```

**See Also:**
- show spantree

# set spantree portcost

Changes the cost that transmission through a network port or ports in the default VLAN on a switch adds to the total cost of a path to the STP root bridge.

**Syntax: set spantree portcost** *port-list* **cost** *cost*

*port-list* List of ports. MSS applies the cost change to all the specified ports.

**cost** *cost* Numeric value. You can specify a value from 1 through 65,535. STP selects lower-cost paths over higher-cost paths.

**Defaults:** The default port cost depends on the port speed and link type. The table below lists the defaults for STP port path cost.

| Port Speed | Link Type | Default Port Path Cost |
|---|---|---|
| 100 Mbps | Full Duplex Aggregate Link (Port Group) | 19 |
| 100 Mbps | Full Duplex | 18 |
| 100 Mbps | Half Duplex | 19 |
| 10 Mbps | Full Duplex Aggregate Link (Port Group) | 19 |
| 10 Mbps | Full Duplex | 95 |
| 10 Mbps | Half Duplex | 100 |

**Access:** Enabled.

**Usage:** This command applies only to the default VLAN (VLAN 1). To change the cost of a port in another VLAN, use the **set spantree portvlancost** command.

**Examples:** The following command changes the cost on ports 3 and 4 to 20:

```
DWS-1008# set spantree portcost 3,4 cost 20
success: change accepted.
```

**See Also:**
- clear spantree portcost
- clear spantree portvlancost
- set spantree portvlancost
- show spantree
- show spantree portvlancost


Download from Www.Somanuals.com. All Manuals Search And Download.

# set spantree portfast

Enables or disables STP port fast convergence on one or more ports on a switch.

**Syntax: set spantree portfast port** *port-list* **{enable | disable}**

**port** *port-list* List of ports. MSS enables the feature on the specified ports.

**enable** Enables port fast convergence.

**disable** Disables port fast convergence.

**Defaults:** STP port fast convergence is disabled by default.

**Access:** Enabled.

**Usage:** Use port fast convergence on ports that are directly connected to servers, hosts, or other MAC stations.

**Examples:** The following command enables port fast convergence on ports 1, 3,and 5:

```
DWS-1008# set spantree portfast port 1,3,5 enable
success: change accepted.
```

**See Also:**
• show spantree portfast

# set spantree portpri

Changes the STP priority of a network port or ports for selection as part of the path to the STP root bridge in the default VLAN on a DWS-1008 switch.

**Syntax: set spantree portpri** *port-list* **priority** *value*

*port-list* List of ports. MSS changes the priority on the specified ports.

**priority** *value* Priority value. You can specify a value from 0 (highest priority) through 255 (lowest priority).

**Defaults:** The default STP priority for all network ports is 128.

**Access:** Enabled.

**Usage:** This command applies only to the default VLAN (VLAN 1). To change the priority of a port in another VLAN, use the **set spantree portvlanpri** command.

**Examples:** The following command sets the priority of ports 3 and 4 to 48:

```
DWS-1008# set spantree portpri 3-4 priority 48
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set spantree portvlancost

Changes the cost of a network port or ports on paths to the STP root bridge for a specific VLAN on an switch.

**Syntax: set spantree portvlancost** *port-list* **cost** *cost* **{all | vlan** *vlan-id***}**

| | |
|---|---|
| *port-list* | List of ports. MSS applies the cost change to all the specified ports. |
| **cost** *cost* | Numeric value. You can specify a value from 1 through 65,535. STP selects lower-cost paths over higher-cost paths. |
| **all** | Changes the cost on all VLANs. |
| **vlan** *vlan-id* | VLAN name or number. MSS changes the cost on only the specified VLAN. |

**Defaults:** The default port cost depends on the port speed and link type.

**Access:** Enabled.

**Examples:** The following command changes the cost on ports 3 and 4 to 20 in VLAN mauve:

```
DWS-1008# set spantree portvlancost 3,4 cost 20 vlan mauve
success: change accepted.
```

**See Also:**
- clear spantree portcost
- clear spantree portvlancost
- set spantree portcost
- show spantree
- show spantree portvlancost

# set spantree portvlanpri

Changes the priority of a network port or ports for selection as part of the path to the STP root bridge, on one VLAN or all VLANs.

**Syntax: set spantree portvlanpri** *port-list* **priority** *value* **{all | vlan** *vlan-id***}**

| | |
|---|---|
| *port-list* | List of ports. MSS changes the priority on the specified ports. |
| **priority** *value* | Priority value. You can specify a value from 0 (highest priority) through 255 (lowest priority). |
| **all** | Changes the priority on all VLANs. |
| **vlan** *vlan-id* | VLAN name or number. MSS changes the priority on only the specified VLAN. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** The default STP priority for all network ports is 128.

**Access:** Enabled.

**Examples:** The following command sets the priority of ports 3 and 4 to 48 on VLAN *mauve*:

```
DWS-1008# set spantree portvlanpri 3-4 priority 48 vlan mauve
success: change accepted.
```

**See Also:**
- clear spantree portpri
- clear spantree portvlanpri
- set spantree portpri
- show spantree

# set spantree priority

Changes the STP root bridge priority of a DWS-1008 switch on one or all of its VLANs.

**Syntax: set spantree priority** *value* **{all | vlan** *vlan-id***}**

| | |
|---|---|
| **priority** *value* | Priority value. You can specify a value from 0 through 65,535. The bridge with the lowest priority value is elected to be the root bridge for the spanning tree. |
| **all** | Changes the bridge priority on all VLANs. |
| **vlan** *vlan-id* | VLAN name or number. MSS changes the bridge priority on only the specified VLAN. |

**Defaults:** The default root bridge priority for the switch on all VLANs is 32,768.

**Access:** Enabled.

**Examples:** The following command sets the bridge priority of VLAN pink to 69:

```
DWS-1008# set spantree priority 69 vlan pink
success: change accepted.
```

**See Also:**
- show spantree


Download from Www.Somanuals.com. All Manuals Search And Download.

# set spantree uplinkfast

Enables or disables STP uplink fast convergence on a switch. This feature enables a switch with redundant links to the network backbone to immediately switch to the backup link to the root bridge if the primary link fails.

**Syntax: set spantree uplinkfast {enable | disable}**

**enable** Enables uplink fast convergence.

**disable** Disables uplink fast convergence.

**Defaults:** Disabled.

**Access:** Enabled.

**Usage:** The uplink fast convergence feature is applicable to bridges that are acting as access switches to the network core (distribution layer) but are not in the core themselves. Do not enable the feature on DWS-1008 switches that are in the network core.

**Examples:** The following command enables uplink fast convergence:

```
DWS-1008# set spantree uplinkfast enable
success: change accepted.
```

**See Also:**
• show spantree uplinkfast

# show spantree

Displays STP configuration and port-state information.

**Syntax: show spantree [port** *port-list* **| vlan** *vlan-id***] [active]**

**port** *port-list* List of ports. If you do not specify any ports, MSS displays STP information for all ports.

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, MSS displays STP information for all VLANs.

**active** Displays information for only the active (forwarding) ports.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** All.

**Examples:** The following command displays STP information for VLAN *default*:

```
DWS-1008# show spantree vlan default
VLAN 1
Spanning Tree Mode          PVST+
Spanning Tree Type          IEEE
Spanning Tree Enabled

Designated Root                     00-02-4a-70-49-f7
Designated Root                     Priority 32768
Designated Root Path Cost           19
Designated Root Port                1
Root Max Age 20 sec       Hello Time 2 sec     Forward Delay 15 sec
Bridge ID MAC ADDR                  00-0b-0e-02-76-f7
Bridge ID Priority                  32768
Bridge Max Age 20 sec     Hello Time 2 sec     Forward Delay 15 sec
Port    Vlan    STP-State     Cost    Prio    Portfast
-------------------------------------------------------------------
1       1       Forwarding    19      128     Disabled
2       1       STP Off       19      128     Disabled
3       1       Disabled      19      128     Disabled
4       1       Disabled      19      128     Disabled
5       1       Disabled      19      128     Disabled
6       1       Disabled      19      128     Disabled
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| VLAN | VLAN number. |
| Spanning Tree Mode | In the current software version, the mode is always PVST+, which means Per VLAN Spanning Tree+. |
| Spanning Tree Type | In the current software version, the type is always IEEE, which means STP is based on the IEEE 802 standards. |
| Spanning Tree Enabled | State of STP on the VLAN. |
| Designated Root | MAC address of the spanning tree's root bridge. |
| Designated Root Priority | Bridge priority of the root bridge. |
| Designated Root Path Cost | Cumulative cost from this bridge to the root bridge. If this switch is the root bridge, then the root cost is 0. |
| Designated Root Port | Port through which this switch reaches the root bridge. If this switch is the root bridge, this field says We are the root. |
| Root Max Age | Maximum acceptable age for hello packets on the root bridge. |
| Root Hello Time | Hello interval on the root bridge. |
| Root Forward Delay | Forwarding delay value on the root bridge. |
| Bridge ID MAC ADDR | This switch's MAC address. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| Bridge ID Priority | This switch's bridge priority. |
| Bridge Max Age | This switch's maximum acceptable age for hello packets. |
| Bridge Hello Time | This switch's hello interval. |
| Bridge Forward Delay | This switch's forwarding delay value. |
| Port | Port number.<br>**Note:** Only network ports are listed. STP does not apply to access point ports or wired authentication ports. |
| Vlan | VLAN ID. |
| STP-State or Port-State | STP state of the port:<br>• Blocking—The port is not forwarding Layer 2 traffic but is listening to and forwarding STP control traffic.<br>• Disabled—This state can indicate any of the following conditions:<br>• The port is inactive.<br>• The port is disabled.<br>• STP is enabled on the port but the port is not forwarding traffic. (The port is active and enabled but STP has just started to come up.)<br>• Forwarding—The port is forwarding Layer 2 traffic.<br>• Learning—The port is learning the locations of other devices in the spanning tree before changing state to forwarding.<br>• Listening—The port is comparing its own STP information with information in STP control packets received by the port to compute the spanning tree and change state to blocking or forwarding.<br>• STP Off—STP is disabled on the port. |
| Cost | STP cost of the port. |
| Prio | STP priority of the port. |
| Portfast | State of the uplink fast convergence feature:<br>• Enabled<br>• Disabled |

**See Also:**

• show spantree blockedports



Download from Www.Somanuals.com. All Manuals Search And Download.

# show spantree backbonefast

Indicates whether the STP backbone fast convergence feature is enabled or disabled.

**Syntax: show spantree backbonefast**

**Defaults:** None.

**Access:** All.

**Examples:** The following example shows the command output on a switch with backbone fast convergence enabled:

```
DWS-1008# show spantree backbonefast
Backbonefast is enabled
```

**See Also:**
• set spantree backbonefast

# show spantree blockedports

Lists information about switch ports that STP has blocked on one or all of its VLANs.

**Syntax: show spantree blockedports [vlan** *vlan-id***]**

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, MSS displays information for blocked ports on all VLANs.

**Defaults:** None.

**Access:** All.

**Usage:** The command lists information separately for each VLAN.

**Examples:** The following command shows information about blocked ports on a switch for the default VLAN (VLAN 1):

```
DWS-1008# show spantree blockedports vlan default
Port     Vlan   Port-State     Cost   Prio    Portfast
-------------------------------------------------------------------
6        190    Blocking       4      128     Disabled
Number of blocked ports (segments) in VLAN 1 : 1
```

The port information is the same as the information displayed by the **show spantree** command.

**See Also:**
• show spantree


Download from Www.Somanuals.com. All Manuals Search And Download.

# show spantree portfast

Displays STP uplink fast convergence information for all network ports or for one or more network ports.

**Syntax: show spantree portfast [***port-list***]**

*port-list* List of ports. If you do not specify any ports, MSS displays uplink fast convergence information for all ports.

**Defaults:** None.

**Access:** All.

**Examples:** The following command shows uplink fast convergence information for all ports:

```
DWS-1008# show spantree portfast
Port    Vlan          Portfast
---------------------------------------
1       1             disable
2       1             disable
3       1             disable
4       1             enable
5       2             disable
6       2             disable
7       2             disable
8       2             disable
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Port | Port number. |
| VLAN | VLAN number. |
| Portfast | State of the uplink fast convergence feature:<br>• Enable<br>• Disable |

**See Also:**
• set spantree portfast


Download from Www.Somanuals.com. All Manuals Search And Download.

# show spantree portvlancost

Displays the cost of a port on a path to the STP root bridge, for each of the port's VLANs.

**Syntax: show spantree portvlancost** *port-list*

*port-list* List of ports.

**Defaults:** None.

**Access:** All.

**Examples:** The following command shows the STP port cost of port 1:

```
DWS-1008# show spantree portvlancost 1
port 1 VLAN 1 have path cost 19
```

**See Also:**
- clear spantree portcost
- clear spantree portvlancost
- set spantree portcost
- set spantree portvlancost
- show spantree

# show spantree statistics

Displays STP statistics for one or more switch network ports.

**Syntax: show spantree statistics [port-list [vlan vlan-id]]**

*port-list* List of ports. If you do not specify any ports, MSS displays STP statistics for all ports.

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, MSS displays STP statistics for all VLANs.

**Defaults:** None.

**Access:** All.

**Usage:** The command displays statistics separately for each port.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command shows STP statistics for port 1:

```
DWS-1008# show spantree statistics 1
BPDU related parameters

Port 1                  VLAN 1
spanning tree enabled for VLAN = 1
port spanning tree                      enabled
state                                   Forwarding
port_id                                 0x8015
port_number                             0x15
path cost                               0x4
message age (port/VLAN)                 0(20)
designated_root                         00-0b-0e-00-04-30
designated cost                         0x0
designated_bridge                       00-0b-0e-00-04-30
designated_port                         38
top_change_ack                          FALSE
config_pending                          FALSE
port_inconsistency                      none

Port based information statistics

config BPDU's xmitted(port/VLAN)        0 (1)
config BPDU's received(port/VLAN)       21825 (43649)
tcn BPDU's xmitted(port/VLAN)           0 (0)
tcn BPDU's received(port/VLAN)          2 (2)
forward transition count (port/VLAN)    1 (1)
scp failure count                       0
root inc trans count (port/VLAN)        1 (1)
inhibit loopguard                       FALSE
loop inc trans count                    0 (0)

Status of Port Timers

forward delay timer                     INACTIVE
forward delay timer value               15
message age timer                       ACTIVE
message age timer value                 0
topology change timer                   INACTIVE
topology change timer value             0
hold timer                              INACTIVE
hold timer value                        0
delay root port timer                   INACTIVE
delay root port timer value             0
delay root port timer restarted is      FALSE
```


Download from Www.Somanuals.com. All Manuals Search And Download.

VLAN based information & statistics

| | |
|---|---|
| spanning tree type | ieee |
| spanning tree multicast address | 01-00-0c-cc-cc-cd |
| bridge priority | 32768 |
| bridge MAC address | 00-0b-0e-12-34-56 |
| bridge hello time | 2 |
| bridge forward delay | 15 |
| topology change initiator: | 0 |
| last topology change occured: | Tue Jul 01 2003 22:33:36. |
| topology change | FALSE |
| topology change time | 35 |
| topology change detected | FALSE |
| topology change count | 1 |
| topology change last recvd. from | 00-0b-0e-02-76-f6 |

Other port specific info

| | |
|---|---|
| dynamic max age transition | 0 |
| port BPDU ok count | 21825 |
| msg age expiry count | 0 |
| link loading | 0 |
| BPDU in processing | FALSE |
| num of similar BPDU's to process | 0 |
| received_inferior_bpdu | FALSE |
| next state | 0 |
| src MAC count | 21807 |
| total src MAC count | 21825 |
| curr_src_mac | 00-0b-0e-00-04-30 |
| next_src_mac | 00-0b-0e-02-76-f6 |

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Port | Port number. |
| VLAN | VLAN ID. |
| Spanning Tree enabled for vlan | State of the STP feature on the VLAN. |
| port spanning tree | State of the STP feature on the port. |
| state | STP state of the port:<br>• Blocking—The port is not forwarding Layer 2 traffic but is listening to and forwarding STP control traffic.<br>• Disabled—The port is not forwarding any traffic, including STP control traffic. The port might be administratively disabled or the link might be disconnected.<br>• Forwarding—The port is forwarding Layer 2 traffic.<br>• Learning—The port is learning the locations of other devices in the spanning tree before changing state to forwarding.<br>• Listening—The port is comparing its own STP information with information in STP control packets received by the port to compute the spanning tree and change state to blocking or forwarding. |
| port_id | STP port ID. |
| port_number | STP port number. |
| path cost | Cost to use this port to reach the root bridge. This is part of the total path cost (designated cost). |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| message age | Age of the protocol information for a port and the value of the maximum age parameter (shown in parenthesis) recorded by the switch. |
| designated_root | MAC address of the root bridge. |
| designated cost | Total path cost to reach the root bridge. |
| designated_bridge | Bridge to which this switch forwards traffic away from the root bridge. |
| designated_port | STP port through which this switch forwards traffic away from the root bridge. |
| top_change_ack | Value of the topology change acknowledgment flag in the next configured bridge protocol data unit (BPDU) to be transmitted on the associated port. The flag is set in reply to a topology change notification BPDU. |
| config_pending | Indicates whether a configured BPDU is to be transmitted on expiration of the hold timer for the port. |
| port_inconsistency | Indicates whether the port is in an inconsistent state. |
| config BPDU's xmitted | Number of BPDUs transmitted from the port. A number in parentheses indicates the number of configured BPDUs transmitted by the switch for this VLAN's spanning tree. |
| config BPDU's received | Number of BPDUs received by this port. A number in parentheses indicates the number of configured BPDUs received by the switch for this VLAN's spanning tree. |
| tcn BPDU's xmitted | Number of topology change notification (TCN) BDPUs transmitted on this port. |
| tcn BPDU's received | Number of TCN BPDUs received on this port. |
| forward transition count | Number of times the port state transitioned to the forwarding state. |
| scp failure count | Number of service control point (SCP) failures. |
| root inc trans count | Number of times the root bridge changed. |
| inhibit loopguard | State of the loop guard. In the current release, the state is always FALSE. |
| loop inc trans count | Number of loops that have occurred. |
| forward delay timer | Status of the forwarding delay timer. This timer monitors the time spent by a port in the listening and learning states. |
| forward delay timer value | Current value of the forwarding delay timer, in seconds. |
| message age timer | Status of the message age timer. This timer measures the age of the received protocol information recorded for a port. |
| message age timer value | Current value of the message age timer, in seconds. |
| topology change timer | Status of the topology change timer. This timer determines the time period during which configured BPDUs are transmitted with the topology change flag set by this switch when it is the root bridge, after detection of a topology change. |
| topology change timer value | Current value of the topology change timer, in seconds. |
| hold timer | Status of the hold timer. This timer ensures that configured BPDUs are not transmitted too frequently through any bridge port. |
| hold timer value | Current value of the hold timer, in seconds. |
| delay root port timer | Status of the delay root port timer, which enables fast convergence when uplink fast convergence is enabled. |
| delay root port timer value | Current value of the delay root port timer. |
| delay root port timer restarted is | Whether the delay root port timer has been restarted. |
| spanning tree type | Type of spanning tree. The type is always IEEE. |
| spanning tree multicast address | Destination address used to send out configured BPDUs on a bridge port. |
| bridge priority | STP priority of this switch. |
| bridge MAC address | MAC address of this switch. |
| bridge hello time | Value of the hello timer interval, in seconds, when this switch is the root or is attempting to become the root. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| bridge forward delay | Value of the forwarding delay interval, in seconds, when this switch is the root or is attempting to become the root. |
| topology change initiator | Port number that initiated the most recent topology change. |
| last topology change occurred | System time when the most recent topology change occurred. |
| topology change | Value of the topology change flag in configuration BPDUs to be transmitted by this switch on VLANs for which the switch is the designated bridge. |
| topology change time | Time period, in seconds, during which BPDUs are transmitted with the topology change flag set by this switch when it is the root bridge, after detection of a topology change. It is equal to the sum of the switch's maximum age and forwarding delay parameters. |
| topology change detected | Indicates whether a topology change has been detected by the switch. |
| topology change count | Number of times the topology change has occurred. |
| topology change last recvd. from | MAC address of the bridge from which the switch last received a topology change. |
| dynamic max age transition | Number of times the maximum age parameter was changed dynamically. |
| port BPDU ok count | Number of valid port BPDUs received. |
| msg age expiry count | Number of expired messages. |
| link loading | Indicates whether the link is oversubscribed. |
| BPDU in processing | Indicates whether BPDUs are currently being processed. |
| num of similar BPDU's to process | Number of similar BPDUs received on a port that need to be processed. |
| received_inferior_bpdu | Indicates whether the port has received an inferior BPDU or a response to a Root Link Query (RLQ) BPDU. |
| next state | Port state before it is set by STP. |
| src MAC count | Number of BPDUs with the same source MAC address. |
| total src MAC count | Number of BPDUs with all the source MAC addresses. |
| curr_src_mac | Source MAC address of the current received BPDU. |
| next_src_mac | Other source MAC address from a different source. |

**See Also:**
• clear spantree statistics

# show spantree uplinkfast

Displays uplink fast convergence information for one VLAN or all VLANs.

**Syntax: show spantree uplinkfast [vlan** *vlan-id***]**

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, MSS displays STP statistics for all VLANs.

**Defaults:** None.

**Access:** All.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command shows uplink fast convergence information for all VLANs:

```
DWS-1008# show spantree uplinkfast
VLAN            port list
----------------------------------------
1               1(fwd),2,3
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| VLAN | VLAN number. |
| port list | Ports in the uplink group. The port that is forwarding traffic is indicated by fwd. The other ports are blocking traffic. |

**See Also:**

- set spantree uplinkfast


Download from Www.Somanuals.com. All Manuals Search And Download.

# IGMP Snooping Commands

Use Internet Group Management Protocol (IGMP) snooping commands to configure and manage multicast traffic reduction on a switch. This chapter presents IGMP snooping commands alphabetically. Use the following table to locate commands in this chapter based on their use.

| | |
|---|---|
| **IGMP Snooping State** | set igmp on page 451<br>show igmp on page 460 |
| **Proxy Reporting** | set igmp proxy-report on page 455 |
| **Pseudo-querier** | set igmp querier on page 458<br>show igmp querier on page 464 |
| **Timers** | set igmp qi on page 456<br>set igmp oqi on page 454<br>set igmp qri on page 457<br>set igmp lmqi on page 452<br>set igmp rv on page 459 |
| **Router Solicitation** | set igmp mrsol on page 453<br>set igmp mrsol mrsi on page 454 |
| **Multicast Routers** | set igmp mrouter on page 452<br>show igmp mrouter on page 462 |
| **Multicast Receivers** | set igmp receiver on page 458<br>show igmp receiver-table on page 465 |
| **Statistics** | show igmp statistics on page 466<br>clear igmp statistics on page 451 |


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear igmp statistics

Clears IGMP statistics counters on one VLAN or all VLANs on a switch and resets them to 0.

**Syntax: clear igmp statistics [vlan** *vlan-id***]**

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, IGMP statistics are cleared for all VLANs.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command clears IGMP statistics for all VLANs:

```
DWS-1008# clear igmp statistics
IGMP statistics cleared for all vlans
```

**See Also:**
• show igmp statistics

# set igmp

Disables or reenables IGMP snooping on one VLAN or all VLANs on a switch.

**Syntax: set igmp {enable | disable} [vlan** *vlan-id***]**

**enable** Enables IGMP snooping.

**disable** Disables IGMP snooping.

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, IGMP snooping is disabled or reenabled on all VLANs.

**Defaults:** IGMP snooping is enabled on all VLANs by default.

**Access:** Enabled.

**Examples:** The following command disables IGMP snooping on VLAN orange:

```
DWS-1008# set igmp disable vlan orange
success: change accepted.
```

**See Also:**
• show igmp


Download from Www.Somanuals.com. All Manuals Search And Download.

# set igmp lmqi

Changes the IGMP last member query interval timer on one VLAN or all VLANs on a switch.

**Syntax: set igmp lmqi** *tenth-seconds* **[vlan** *vlan-id***]**

| | |
|---|---|
| **lmqi** *tenth-seconds* | Amount of time (in tenths of a second) that the switch waits for a response to a group-specific query after receiving a leave message for that group, before removing the receiver that sent the leave message from the list of receivers for the group. If there are no more receivers for the group, the switch also sends a leave message for the group to multicast routers. You can specify a value from 1 through 65,535. |
| **vlan** *vlan-id* | VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs. |

**Defaults:** The default last member query interval is 10 tenths of a second (1 second).

**Access:** Enabled.

**Examples:** The following command changes the last member query interval on VLAN orange to 5 tenths of a second:

```
DWS-1008# set igmp lmqi 5 vlan orange
success: change accepted.
```

**See Also:**
- set igmp oqi
- set igmp qi
- set igmp mrouter

# set igmp mrouter

Adds or removes a port in a switch's list of ports on which it forwards traffic to multicast routers. Static multicast ports are immediately added to or removed from the list of router ports and do not age out.

**Syntax: set igmp mrouter port** *port-list* **{enable | disable}**

| | |
|---|---|
| **port** *port-list* | Port list. MSS adds or removes the specified ports in the list of static multicast router ports. |
| **enable** | Adds the port to the list of static multicast router ports. |
| **disable** | Removes the port from the list of static multicast router ports. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** By default, no ports are static multicast router ports.

**Access:** Enabled.

**Usage:** You cannot add AP access ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

**Examples:** The following command adds port 5 as a static multicast router port:

```
DWS-1008# set igmp mrouter port 5 enable
success: change accepted.
```

The following command removes port 5 from the static multicast router port list:

```
DWS-1008# set igmp mrouter port 5 disable
success: change accepted.
```

**See Also:**
• show igmp mrouter

# set igmp mrsol

Enables or disables multicast router solicitation by a switch on one VLAN or all VLANs.

**Syntax: set igmp mrsol {enable | disable} [vlan** *vlan-id***]**

| | |
|---|---|
| **enable** | Enables multicast router solicitation. |
| **disable** | Disables multicast router solicitation. |
| **vlan** *vlan-id* | VLAN name or number. If you do not specify a VLAN, multicast router solicitation is disabled or enabled on all VLANs. |

**Defaults:** Multicast router solicitation is disabled on all VLANs by default.

**Access:** Enabled.

**Examples:** The following command enables multicast router solicitation on VLAN *orange*:

```
DWS-1008# set igmp mrsol enable vlan orange
success: change accepted.
```

**See Also:**
• set igmp mrsol mrsi


Download from Www.Somanuals.com. All Manuals Search And Download.

# set igmp mrsol mrsi

Changes the interval between multicast router solicitations by a switch on one VLAN or all VLANs.

**Syntax: set igmp mrsol mrsi** *seconds* **[vlan** *vlan-id***]**

| | |
|---|---|
| *seconds* | Number of seconds between multicast router solicitations. You can specify a value from 1 through 65,535. |
| **vlan** *vlan-id* | VLAN name or number. If you do not specify a VLAN, MSS changes the multicast router solicitation interval for all VLANs. |

**Defaults:** The interval between multicast router solicitations is 30 seconds by default.

**Access:** Enabled.

**Examples:** The following example changes the multicast router solicitation interval to 60 seconds:

```
DWS-1008# set igmp mrsol mrsi 60
success: change accepted.
```

**See Also:**
• set igmp mrsol

# set igmp oqi

Changes the IGMP other-querier-present interval timer on one VLAN or all VLANs on a switch.

**Syntax: set igmp oqi** *seconds* **[vlan** *vlan-id***]**

| | |
|---|---|
| **oqi** *seconds* | Number of seconds that the switch waits for a general query to arrive before electing itself the querier. You can specify a value from 1 through 65,535. |
| **vlan** *vlan-id* | VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs. |

**Defaults:** The default other-querier-present interval is 255 seconds (4.25 minutes).

**Access:** Enabled.

**Usage:** A switch cannot become the querier unless the pseudo-querier feature is enabled on the switch. When the feature is enabled, the switch becomes the querier for a subnet so long as the switch does not receive a query message from a router with a lower IP address than the IP address of the switch in that subnet. To enable the pseudo-querier feature, use **set igmp querier**.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command changes the other-querier-present interval on VLAN orange to 200 seconds:

```
DWS-1008# set igmp oqi 200 vlan orange
success: change accepted.
```

**See Also:**
- set igmp lmqi
- set igmp qi
- set igmp qri
- set igmp querier
- set igmp mrouter
- set igmp rv

# set igmp proxy-report

Disables or reenables proxy reporting by a switch on one VLAN or all VLANs.

**Syntax: set igmp proxy-report {enable | disable} [vlan** *vlan-id***]**

**enable** Enables proxy reporting.

**disable** Disables proxy reporting.

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, proxy reporting is disabled or reenabled on all VLANs.

**Defaults:** Proxy reporting is enabled on all VLANs by default.

**Access:** Enabled.

**Usage:** Proxy reporting reduces multicast overhead by sending only one membership report for a group to the multicast routers and discarding other membership reports for the same group. If you disable proxy reporting, the switch sends all membership reports to the routers, including multiple reports for the same group.

**Examples:** The following example disables proxy reporting on VLAN *orange*:

```
DWS-1008# set igmp proxy-report disable vlan orange
success: change accepted.
```

**See Also:**
- show igmp


Download from Www.Somanuals.com. All Manuals Search And Download.

# set igmp qi

Changes the IGMP query interval timer on one VLAN or all VLANs on a switch.

**Syntax: set igmp qi** *seconds* **[vlan** *vlan-id***]**

| | |
|---|---|
| **qi** *seconds* | Number of seconds that elapse between general queries sent by the switch when the switch is the querier for the subnet. You can specify a value from 1 through 65,535. |
| **vlan** *vlan-id* | VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs. |

**Defaults:** The default query interval is 125 seconds.

**Access:** Enabled.

**Usage:** The query interval is applicable only when the switch is querier for the subnet. For the switch to become the querier, the pseudo-querier feature must be enabled on the switch and the switch must have the lowest IP address among all the devices eligible to become a querier. To enable the pseudo-querier feature, use the **set igmp querier** command.

**Examples:** The following command changes the query interval on VLAN *orange* to 100 seconds:

```
DWS-1008# set igmp qi 100 vlan orange
success: change accepted.
```

**See Also:**
- set igmp lmqi
- set igmp oqi
- set igmp qri
- set igmp querier
- set igmp mrouter
- set igmp rv


Download from Www.Somanuals.com. All Manuals Search And Download.

# set igmp qri

Changes the IGMP query response interval timer on one VLAN or all VLANs on a switch.

**Syntax: set igmp qri** *tenth-seconds* **[vlan** *vlan-id***]**

**qri** *tenth-seconds* Amount of time (in tenths of a second) that the switch waits for a receiver to respond to a group-specific query message before removing the receiver from the receiver list for the group. You can specify a value from 1 through 65,535.

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

**Defaults:** The default query response interval is 100 tenths of a second (10 seconds).

**Access:** Enabled.

**Usage:** The query response interval is applicable only when the switch is querier for the subnet. For the switch to become the querier, the pseudo-querier feature must be enabled on the switch and the switch must have the lowest IP address among all the devices eligible to become a querier. To enable the pseudo-querier feature, use **set igmp querier**.

**Examples:** The following command changes the query response interval on VLAN *orange* to 50 tenths of a second (5 seconds):

```
DWS-1008# set igmp qri 50 vlan orange
success: change accepted.
```

**See Also:**
- set igmp lmqi
- set igmp oqi
- set igmp qi
- set igmp querier
- set igmp rv


Download from Www.Somanuals.com. All Manuals Search And Download.

# set igmp querier

Enables or disables the IGMP pseudo-querier on a DWS-1008 switch, on one VLAN or all VLANs.

**Syntax: set igmp querier {enable | disable} [vlan** *vlan-id***]**

**enable** Enables the pseudo-querier.

**disable** Disables the pseudo-querier.

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, the pseudo-querier is enabled or disabled on all VLANs.

**Defaults:** The pseudo-querier is disabled on all VLANs by default.

**Access:** Enabled.

**Usage:** D-Link recommends that you use the pseudo-querier only when the VLAN contains local multicast traffic sources and no multicast router is servicing the subnet.

**Examples:** The following example enables the pseudo-querier on the orange VLAN:

```
DWS-1008# set igmp querier enable vlan orange
success: change accepted.
```

**See Also:**
• show igmp querier

# set igmp receiver

Adds or removes a network port in the list of ports on which a switch forwards traffic to multicast receivers. Static multicast receiver ports are immediately added to or removed from the list of receiver ports and do not age out.

**Syntax: set igmp receiver port** *port-list* **{enable | disable}**

**port** *port-list* Network port list. MSS adds the specified ports to the list of static multicast receiver ports.

**enable** Adds the port to the list of static multicast receiver ports.

**disable** Removes the port from the list of static multicast receiver ports.

**Defaults:** By default, no ports are static multicast receiver ports.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** You cannot add AP access ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

**Examples:** The following command adds port 7 as a static multicast receiver port:

```
DWS-1008# set igmp receiver port 7 enable
success: change accepted.
```

The following command removes port 4 from the list of static multicast receiver ports:

```
DWS-1008# set igmp receiver port 4 disable
success: change accepted.
```

**See Also:**
- show igmp receiver-table

# set igmp rv

Changes the robustness value for one VLAN or all VLANs on a DWS-1008 switch. Robustness adjusts the IGMP timers to the amount of traffic loss that occurs on the network.

**Syntax: set igmp rv** *num* **[vlan vlan-id]**

| | |
|---|---|
| *num* | Robustness value. You can specify a value from 2 through 255. Set the robustness value higher to adjust for more traffic loss. |
| **vlan** *vlan-id* | VLAN name or number. If you do not specify a VLAN, MSS changes the robustness value for all VLANs. |

**Defaults:** The default robustness value for all VLANs is 2.

**Access:** Enabled.

**Examples:** The following example changes the robustness value on VLAN *orange* to 4:

```
DWS-1008# set igmp rv 4 vlan orange
success: change accepted.
```

**See Also:**
- set igmp oqi
- set igmp qi
- set igmp qri


Download from Www.Somanuals.com. All Manuals Search And Download.

# show igmp

Displays IGMP configuration information and statistics for one VLAN or all VLANs.

**Syntax: show igmp [vlan vlan-id]**

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, MSS displays IGMP information for all VLANs.

**Defaults:** None.

**Access:** All.

**Examples:** The following command displays IGMP information for VLAN orange:

```
DWS-1008# show igmp vlan orange
VLAN: orange
IGMP is enabled
Proxy reporting is on
Mrouter solicitation is on
Querier functionality is off
Configuration values: qi: 125 oqi: 300 qri: 100 lmqi: 10 rvalue: 2
Multicast
router information:
Port    Mrouter-IPaddr      Mrouter-MAC         Type          TTL
-------------------------------------------------------------------------------------------
5       192.28.7.5          00:01:02:03:04:05   dvmrp         17
Group                 Port  Receiver-IP         Receiver-MAC        TTL
-------------------------------------------------------------------------------------------
224.0.0.2             none  none                none                undef
237.255.255.255       5     10.10.10.11         00:02:04:06:08:0b   258
237.255.255.255       5     10.10.10.13         00:02:04:06:08:0d   258
237.255.255.255       5     10.10.10.14         00:02:04:06:08:0e   258
237.255.255.255       5     10.10.10.12         00:02:04:06:08:0c   258
237.255.255.255       5     10.10.10.10         00:02:04:06:08:0a   258
Querier information:
Querier for vlan orange
Port    Querier-IP          Querier-MAC         TTL
-------------------------------------------------------------------
1       193.122.135.178     00:0b:cc:d2:e9:b4   23

IGMP vlan member ports: 2,4,5,6,7,8
IGMP static ports: none
IGMP statistics for vlan orange:
```


Download from Www.Somanuals.com. All Manuals Search And Download.

```
IGMP message type        Received    Transmitted  Dropped
-------------------------------------------------------------------------------
General-Queries          0           0            0
GS-Queries               0           0            0
Report V1                0           0            0
Report V2                5           1            4
Leave                    0           0            0
Mrouter-Adv              0           0            0
Mrouter-Term             0           0            0
Mrouter-Sol              50          101          0
DVMRP                    4           4            0
PIM V1                   0           0            0
PIM V2                   0           0            0
Topology notifications: 0
Packets with unknown IGMP type: 0
Packets with bad length: 0
Packets with bad checksum: 0
Packets dropped: 4
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| VLAN | VLAN name. MSS displays information separately for each VLAN. |
| IGMP is enabled (disabled) | IGMP state. |
| Proxy reporting | Proxy reporting state. |
| Mrouter solicitation | Multicast router solicitation state. |
| Querier functionality | Pseudo-querier state. |
| Configuration values (qi) | Query interval. |
| Configuration values (oqi) | Other-querier-present interval. |
| Configuration values (qri) | Query response interval. |
| Configuration values (lmqi) | Last member query interval. |
| Configuration values (rvalue) | Robustness value. |
| Multicast router information | List of multicast routers and active multicast groups. The fields containing this information are described separately. The show igmp mrouter command shows the same information. |
| Port | Number of the physical port through which the switch can reach the router. |
| Mrouter-IPaddr | IP address of the multicast router interface. |
| Mrouter-MAC | MAC address of the multicast router interface. |
| Type | How the switch learned that the port is a multicast router port:<br>• conf — Static multicast port configured by an administrator<br>• madv—Multicast advertisement<br>• quer—IGMP query<br>• dvmrp—Distance Vector Multicast Routing Protocol (DVMRP)<br>• pimv1—Protocol Independent Multicast (PIM) version 1<br>• pimv2—PIM version 2 |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| TTL | Number of seconds before this entry ages out if not refreshed. For static multicast router entries, the time-to-live (TTL) value is undef. Static multicast router entries do not age out. |
| Group | IP address of a multicast group. The **show igmp receiver-table** command shows the same information as these receiver fields. |
| Port | Physical port through which the switch can reach the group's receiver. |
| Receiver-IP | IP address of the client receiving the group. |
| Receiver-MAC | MAC address of the client receiving the group. |
| TTL | Number of seconds before this entry ages out if the switch does not receive a group membership message from the receiver. For static multicast receiver entries, the TTL value is undef. Static multicast receiver entries do not age out. |
| Querier information | Information about the subnet's multicast querier. If the querier is another device, the fields described below are applicable. If the querier is the switch itself, the output indicates how many seconds remain until the next general query message. If IGMP snooping does not detect a querier, the output indicates this. The **show igmp querier** command shows the same information. |
| Querier for vlan | VLAN containing the querier. Information is listed separately for each VLAN. |
| Querier-IP | IP address of the querier. |
| Querier-MAC | MAC address of the querier. |
| TTL | Number of seconds before this entry ages out if the switch does not receive a query message from the querier. |
| IGMP vlan member ports | Physical ports in the VLAN. This list includes all network ports configured to be in the VLAN and all ports MSS dynamically assigns to the VLAN when a user assigned to the VLAN becomes a receiver. For example, the list can include an AP access port that is not configured to be in the VLAN when a user associated with the access point on that port becomes a receiver for a group. When all receivers on a dynamically added port age out, MSS removes the port from the list. |
| IGMP static ports | Static receiver ports. |
| IGMP statistics | Multicast message and packet statistics. These are the same statistics displayed by the show igmp statistics command. |

**See Also:**
- show igmp mrouter
- show igmp querier
- show igmp receiver-table
- show igmp statistics

# show igmp mrouter

Displays the multicast routers in a switch's subnet, on one VLAN or all VLANs. Routers are listed separately for each VLAN, according to the port number through which the switch can reach the router.

**Syntax: show igmp mrouter [vlan** *vlan-id***]**


Download from Www.Somanuals.com. All Manuals Search And Download.

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, MSS displays the multicast routers in all VLANs.

**Defaults:** None.

**Access:** All.

**Examples:** The following command displays the multicast routers in VLAN orange:

```
DWS-1008# show igmp mrouter vlan orange
Multicast routers for vlan orange
Port    Mrouter-IPaddr      Mrouter-MAC         Type        TTL
-------------------------------------------------------------------------------
10      192.28.7.5          00:01:02:03:04:05   dvmrp       33
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Multicast routers for vlan | VLAN containing the multicast routers. Ports are listed separately for each VLAN. |
| Port | Number of the physical port through which the switch can reach the router. |
| Mrouter-IPaddr | IP address of the multicast router. |
| Mrouter-MAC | MAC address of the multicast router. |
| Type | How the switch learned that the port is a multicast router port:<br>• conf — Static multicast port configured by an administrator<br>• madv—Multicast advertisement<br>• quer—IGMP query<br>• dvmrp—Distance Vector Multicast Routing Protocol (DVMRP)<br>• pimv1—Protocol Independent Multicast (PIM) version 1<br>• pimv2—PIM version 2 |
| TTL | Number of seconds before this entry ages out if unused. For static multicast router entries, the TTL value is *undef*. Static multicast router entries do not age out. |

**See Also:**
- set igmp mrouter
- show igmp mrouter


Download from Www.Somanuals.com. All Manuals Search And Download.

# show igmp querier

Displays information about the active multicast querier, on one VLAN or all VLANs. Queriers are listed separately for each VLAN. Each VLAN can have only one querier.

**Syntax: show igmp querier [vlan** *vlan-id***]**

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, MSS displays querier information for all VLANs.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command displays querier information for VLAN orange:

```
DWS-1008# show igmp querier vlan orange
Querier for vlan orange
Port    Querier-IP          Querier-MAC        TTL
-------------------------------------------------------------------
1       193.122.135.178     00:0b:cc:d2:e9:b4  23
```

The following command shows the information MSS displays when the querier is the switch itself:

```
DWS-1008# show igmp querier vlan default
Querier for vlan default:
I am the querier for vlan default, time to next query is 20
```

The output indicates how many seconds remain before the pseudo-querier on the switch broadcasts the next general query report to IP address 224.0.0.1, the multicast all-systems group.

If IGMP snooping does not detect a querier, the output indicates this finding, as shown in the following example:

```
DWS-1008# show igmp querier vlan red
Querier for vlan red:
There is no querier present on vlan red
```

This condition does not necessarily indicate a problem. For example, election of the querier might be in progress.


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields in the display when a querier other than the switch is present.

| Field | Description |
|---|---|
| Querier for vlan | VLAN containing the querier. Information is listed separately for each VLAN. |
| Querier-IP | IP address of the querier interface. |
| Querier-MAC | MAC address of the querier interface. |
| TTL | Number of seconds before this entry ages out if the switch does not receive a query message from the querier. |

**See Also:**
• set igmp querier

# show igmp receiver-table

Displays the receivers to which a switch forwards multicast traffic. You can display receivers for all VLANs, a single VLAN, or a group or groups identified by group address and network mask.

**Syntax: show igmp receiver-table [vlan** *vlan-id***] [group** *group-ip-addr/mask-length***]**

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, MSS displays the multicast receivers on all VLANs.

**group** *group-ip-addr/mask-length* IP address and subnet mask of a multicast group, in CIDR format (for example, 239.20.20.10/24). If you do not specify a group address, MSS displays the multicast receivers for all groups.

**Defaults:** None.

**Access:** All.

**Examples:** The following command displays all multicast receivers in VLAN orange:

```
DWS-1008# show igmp receiver-table vlan orange
VLAN: orange
Session              Port   Receiver-IP   Receiver-MAC       TTL
-------------------------------------------------------------------------------
224.0.0.2            none   none          none               undef
237.255.255.255      5      10.10.10.11   00:02:04:06:08:0b  179
237.255.255.255      5      10.10.10.13   00:02:04:06:08:0d  179
237.255.255.255      5      10.10.10.14   00:02:04:06:08:0e  179
237.255.255.255      5      10.10.10.12   00:02:04:06:08:0c  179
237.255.255.255      5      10.10.10.10   00:02:04:06:08:0a  179
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The following command lists all receivers for multicast groups 237.255.255.1 through 237.255.255.255, in all VLANs:

```
DWS-1008# show igmp receiver-table group 237.255.255.0/24
VLAN: red
Session              Port   Receiver-IP   Receiver-MAC       TTL
-------------------------------------------------------------------------------
237.255.255.2        2      10.10.20.19   00:02:04:06:09:0d  112
237.255.255.119      3      10.10.30.31   00:02:04:06:01:0b  112

VLAN: green
Session              Port   Receiver-IP   Receiver-MAC       TTL
-------------------------------------------------------------------------------
237.255.255.17       11     10.10.40.41   00:02:06:08:02:0c  12
237.255.255.255      6      10.10.60.61   00:05:09:0c:0a:01  111
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| VLAN | VLAN that contains the multicast receiver ports. Ports are listed separately for each VLAN. |
| Session | IP address of the multicast group being received. |
| Port | Physical port through which the switch can reach the receiver. |
| Receiver-IP | IP address of the receiver. |
| Receiver-MAC | MAC address of the receiver. |
| TTL | Number of seconds before this entry ages out if the switch does not receive a group membership message from the receiver. For static multicast receiver entries, the TTL value is *undef*. Static multicast receiver entries do not age out. |

**See Also:**
• set igmp receiver

# show igmp statistics

Displays IGMP statistics.

**Syntax: show igmp statistics [vlan** *vlan-id***]**

**vlan** *vlan-id* VLAN name or number. If you do not specify a VLAN, MSS displays IGMP statistics for all VLANs.

**Defaults:** None.

**Access:** All.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command displays IGMP statistics for VLAN *orange*:

```
DWS-1008# show igmp statistics vlan orange
IGMP statistics for vlan orange:
IGMP message type          Received    Transmitted  Dropped
-------------------------------------------------------------------------------
General-Queries            0           0            0
GS-Queries                 0           0            0
Report V1                  0           0            0
Report V2                  5           1            4
Leave                      0           0            0
Mrouter-Adv                0           0            0
Mrouter-Term               0           0            0
Mrouter-Sol                50          101          0
DVMRP                      4           4            0
PIM V1                     0           0            0
PIM V2                     0           0            0
Topology notifications: 0
Packets with unknown IGMP type: 0
Packets with bad length: 0
Packets with bad checksum: 0
Packets dropped: 4
```

The table below describes the fields in this display.

| Field | Description |
|---|---|
| IGMP statistics for vlan | VLAN name. Statistics are listed separately for each VLAN. |
| IGMP message type | Type of IGMP message:<br>• General-Queries—General group membership queries sent by the multicast querier (multicast router or pseudo-querier).<br>• GS-Queries—Group-specific queries sent by the the multicast querier to determine whether there are receivers for a specific group.<br>• Report V1—IGMP version 1 group membership reports sent by clients who want to be receivers for the groups.<br>• Report V2—IGMP version 2 group membership reports sent by clients who want to be receivers for the groups.<br>• Leave—IGMP version 2 leave messages sent by clients who want to stop receiving traffic for a group. Leave messages apply only to IGMP version 2.<br>• Mrouter-Adv—Multicast router advertisement packets. A multicast router sends this type of packet to advertise the IP address of the sending interface as a multicast router interface. |
| IGMP message type | Type of IGMP message, continued:<br>• Mrouter-Term—Multicast router termination messages. A multicast router sends this type of message when multicast forwarding is disabled on the router interface, the router interface is administratively disabled, or the router itself is gracefully shutdown.<br>• Mrouter-Sol—Multicast router solicitation messages. A multicast client or a switch sends this type of message to immediately solicit multicast router advertisement messages from the multicast routers in the subnet.<br>• DVMRP—Distance Vector Multicast Routing Protocol (DVMRP) messages. Multicast routers running DVMRP exchange multicast information with these messages.<br>• PIM V1—Protocol Independent Multicast (PIM) version 1 messages. Multicast routers running PIMv1 exchange multicast information with these messages.<br>• PIM V2—PIM version 2 messages. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| Received | Number of packets received. |
| Transmitted | Number of packets transmitted. This number includes both multicast packets originated by the switch and multicast packets received and then forwarded by the switch. |
| Dropped | Number of IGMP packets dropped by the switch. |
| Topology notifications | Number of Layer 2 topology change notifications received by the switch.<br>**Note:** In the current software version, the value in this field is always 0. |
| Packets with unknown IGMP type | Number of multicast packets received with an unrecognized multicast type. |
| Packets with bad length | Number of packets with an invalid length. |
| Packets with bad IGMP checksum | Number of packets with an invalid IGMP checksum value. |
| Packets dropped | Number of multicast packets dropped by the switch. |

**See Also:**

- clear igmp statistics



Download from Www.Somanuals.com. All Manuals Search And Download.

# Security ACL Commands

Use security ACL commands to configure and monitor security access control lists (ACLs). Security ACLs filter packets to restrict or permit network usage by certain users or traffic types, and can assign to packets a class of service (CoS) to define the priority of treatment for packet filtering. (Security ACLs are different from the location policy on a DWS-1008 switch, which helps you locally control user access.

This chapter presents security ACL commands alphabetically. Use the following table to locate commands in this chapter based on their use.


| | |
|---|---|
| **Create Security ACLs** | clear security acl on page 470<br>set security acl on page 475<br>show security acl on page 482<br>show security acl editbuffer on page 483<br>show security acl info on page 484 |
| **Commit Security ACLs** | commit security acl on page 472<br>rollback security acl on page 474 |
| **Map Security ACLs** | clear security acl map on page 471<br>set security acl map on page 479<br>show security acl map on page 486 |
| **Monitor Security ACLs** | set security acl hit-sample-rate on page 481<br>show security acl hits on page 484<br>show security acl resource-usage on page 486 |




Download from Www.Somanuals.com. All Manuals Search And Download.

# clear security acl

Clears a specified security ACL, an access control entry (ACE), or all security ACLs, from the edit buffer. When used with the command **commit security acl**, clears the ACE from the running configuration.

**Syntax: clear security acl {***acl-name* **| all} [***editbuffer-index***]**

| | |
|---|---|
| *acl-name* | Name of an existing security ACL to clear. ACL names start with a letter and are case-insensitive. |
| **all** | Clears all security ACLs. |
| *editbuffer-index* | Number that indicates which access control entry (ACE) in the security ACL to clear. If you do not specify an ACE, all ACEs are cleared from the ACL. |

**Defaults:** None.

**Access:** Enabled.

**Usage:** This command deletes security ACLs only in the edit buffer. You must use the **commit security acl** command with this command to delete the ACL or ACE from the running configuration and nonvolatile storage.

The **clear security acl** command deletes a security ACL, but does not stop its current filtering function if the ACL is mapped to any virtual LANs (VLANs), ports, or virtual ports, or if the ACL is applied in a Filter-Id attribute to an authenticated user or group of users with current sessions.

**Examples:** The following commands display the current security ACL configuration, clear acl_133 in the edit buffer, commit the deletion to the running configuration, and redisplay the ACL configuration to show that it no longer contains acl_133:

```
DWS-1008# show security acl info all
ACL information for all
set security acl ip acl_133 (hits #1 0)
---------------------------------------------------------
1. deny IP source IP 192.168.1.6 0.0.0.0 destination IP any
set security acl ip acl_134 (hits #3 0)
---------------------------------------------------------
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
---------------------------------------------------------
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits

DWS-1008# clear security acl acl_133

DWS-1008# commit security acl acl_133
configuration accepted
```


Download from Www.Somanuals.com. All Manuals Search And Download.

```
DWS-1008# show security acl info all
ACL information for all
set security acl ip acl_134 (hits #3 0)
---------------------------------------------------------
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
---------------------------------------------------------
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
```

**See Also:**
- clear security acl map
- commit security acl
- set security acl
- show security acl info

# clear security acl map

Deletes the mapping between a security ACL and a virtual LAN (VLAN), one or more physical ports, or a virtual port. Or deletes all ACL maps to VLANs, ports, and virtual ports on a switch.

**Note:** Security ACLs are applied to users or groups dynamically via the Filter-Id attribute. To delete a security ACL from a user or group in the local database, use the command **clear user attr**, **clear mac-user attr**, **clear usergroup attr**, or **clear mac-usergroup attr**. To delete a security ACL from a user or group on an external RADIUS server, see the documentation for your RADIUS server.

**Syntax: clear security acl map {***acl-name* **| all} {vlan** *vlan-id* **| port** *port-list* **[tag** *tag-value***] | dap** *dap-num***} {in | out}**

| | |
|---|---|
| *acl-name* | Name of an existing security ACL to clear. ACL names start with a letter and are case-insensitive. |
| **all** | Removes security ACL mapping from all physical ports, virtual ports, and VLANs on an switch. |
| **vlan** *vlan-id* | VLAN name or number. MSS removes the security ACL from the specified VLAN. |
| **port** *port-list* | Port list. MSS removes the security ACL from the specified physical port or ports. |
| **tag** *tag-value* | Tag value that identifies a virtual port in a VLAN. Specify a value from 1 through 4095. MSS removes the security ACL from the specified virtual port. |
| **dap** *dap-num* | One or more Distributed APs, based on their connection IDs. Specify a single connection ID, or specify a comma-separated list of connection IDs, a hyphen-separated range, or any combination, with no spaces. MSS removes the security ACL from the specified Distributed APs. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**in** Removes the security ACL from traffic coming into the switch.

**out** Removes the security ACL from traffic going out of the switch.

**Defaults:** None.

**Access:** Enabled.

**Usage:** To clear a security ACL map, type the name of the ACL with the VLAN, physical port or ports, virtual port tag, or Distributed AP and the direction of the packets to stop filtering. This command deletes the ACL mapping, but not the ACL.

**Examples:** To clear the mapping of security ACL acljoe from port 4 for incoming packets, type the following command:

```
DWS-1008# clear security acl map acljoe port 4 in
clear mapping accepted
```

To clear all physical ports, virtual ports, and VLANs on a switch of the ACLs mapped for incoming and outgoing traffic, type the following command:

```
DWS-1008# clear security acl map all
success: change accepted.
```

**See Also:**
- clear security acl
- set security acl map
- show security acl map

# commit security acl

Saves a security ACL, or all security ACLs, in the edit buffer to the running configuration and nonvolatile storage on the switch. Or, when used with the **clear security acl** command, commit security acl deletes a security ACL, or all security ACLs, from the running configuration and nonvolatile storage.

**Syntax: commit security acl {***acl-name* **| all}**

*acl-name* Name of an existing security ACL to commit. ACL names must start with a letter and are case-insensitive.

**all** Commits all security ACLs in the edit buffer.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** Enabled.

**Usage:** Use the **commit security acl** command to save security ACLs into, or delete them from, the permanent configuration. Until you commit the creation or deletion of a security ACL, it is stored in an edit buffer and is not enforced. After you commit a security ACL, it is removed from the edit buffer.

A single **commit security acl all** command commits the creation and/or deletion of whatever show security acl info all editbuffer shows to be currently stored in the edit buffer.

**Examples:** The following commands commit all the security ACLs in the edit buffer to the configuration, display a summary of the committed ACLs, and show that the edit buffer has been cleared:

```
DWS-1008# commit security acl all
configuration accepted

DWS-1008# show security acl
ACL table
ACL             Type   Class  Mapping
-------------------------------------------------
acl_123         IP     Static
acl_124         IP     Static

DWS-1008# show security acl info all editbuffer
acl editbuffer information for all
```

**See Also:**
- clear security acl
- rollback security acl
- set security acl
- show security acl
- show security acl info


Download from Www.Somanuals.com. All Manuals Search And Download.

# rollback security acl

Clears changes made to the security ACL edit buffer since it was last saved. The ACL is rolled back to its state after the last **commit security acl** command was entered. All uncommitted ACLs in the edit buffer are cleared.

**Syntax: rollback security acl {***acl-name* **| all}**

*acl-name* Name of an existing security ACL to roll back. ACL names must start with a letter and are case-insensitive.

**all** Rolls back all security ACLs in the edit buffer, clearing all uncommitted ACEs.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following commands show the edit buffer before a rollback, clear any changes in the edit buffer to security acl_122, and show the edit buffer after the rollback:

```
DWS-1008# show security acl info all editbuffer
ACL edit-buffer information for all

set security acl ip acl_122 (ACEs 3, add 3, del 0, modified 0)
---------------------------------------------------------------------------------------------
1. permit IP source IP 20.0.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 20.0.2.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.1.234 255.255.255.255 enable-hits

DWS-1008# rollback security acl acl_122

DWS-1008# show security acl info all editbuffer
ACL edit-buffer information for all
```

**See Also:**
- show security acl


Download from Www.Somanuals.com. All Manuals Search And Download.

# set security acl

In the edit buffer, creates a security access control list (ACL), adds one access control entry (ACE) to a security ACL, and/or reorders ACEs in the ACL. The ACEs in an ACL filter IP packets by source IP address, a Layer 4 protocol, or IP, ICMP, TCP, or UDP packet information.

**Syntax**

**By source address**

**set security acl ip** *acl-name* **{permit [cos** *cos*] **| deny}** {*source-ip-addr mask* **| any}**
**[before** *editbuffer-index* **| modify** *editbuffer-index*] **[hits]**

**By Layer 4 protocol**

**set security acl ip** *acl-name* **{permit [cos** *cos*] **| deny}** *protocol-number*
{*source-ip-addr mask* **| any}** {*destination-ip-addr mask* **| any}**
**[[precedence** *precedence*] **[tos** *tos*] **| [dscp** *codepoint*]]
**[before** *editbuffer-index* **| modify** *editbuffer-index*] **[hits]**

**By IP packets**

**set security acl ip** *acl-name* **{permit [cos** *cos*] **| deny}**
**ip** {*source-ip-addr mask* **| any}** {*destination-ip-addr mask* **| any}**
**[[precedence** *precedence*] **[tos** *tos*] **| [dscp** *codepoint*]]
**[before** *editbuffer-index* **| modify** *editbuffer-index*] **[hits]**

**By ICMP packets**

**set security acl ip** *acl-name* **{permit [cos** *cos*] **| deny}**
**icmp** {*source-ip-addr mask* **| any}** {*destination-ip-addr mask* **| any}**
**[type** *icmp-type*] **[code** *icmp-code*]
**[[precedence** *precedence*] **[tos** *tos*] **| [dscp** *codepoint*]]
**[before** *editbuffer-index* **| modify** *editbuffer-index*] **[hits]**

**By TCP packets**

**set security acl ip** *acl-name* **{permit [cos** *cos*] **| deny}**
**tcp** {*source-ip-addr mask* **| any [***operator port* **[***port2*]]}
{*destination-ip-addr mask* **| any [***operator port* **[***port2*]]}
**[[precedence** *precedence*] **[tos** *tos*] **| [dscp** *codepoint*]]
**[established] [before** *editbuffer-index* **| modify** *editbuffer-index*] **[hits]**

**By UDP packets**

**set security acl ip** *acl-name* **{permit [cos** *cos*] **| deny}**
**udp** {*source-ip-addr mask* **| any [***operator port* **[***port2*]]}
{*destination-ip-addr mask* **| any [***operator port* **[***port2*]]}
**[[precedence** *precedence*] **[tos** *tos*] **| [dscp** *codepoint*]]
**[before** *editbuffer-index* **| modify** *editbuffer-index*] **[hits]**


Download from Www.Somanuals.com. All Manuals Search And Download.

*acl-name* Security ACL name. ACL names must be unique within the switch, must start with a letter, and are case-insensitive. Specify an ACL name of up to 32 of the following characters:

- Letters a through z and A through Z
- Numbers 0 through 9
- Hyphen (-), underscore (_), and period (.)

D-Link recommends that you do not use the same name with different capitalizations for ACLs. For example, do not configure two separate ACLs with the names acl_123 and ACL_123.

**Note:** In an ACL name, do not include the term all, default-action, map, help, or editbuffer.

**permit** Allows traffic that matches the conditions in the ACE.

**cos** *cos* For permitted packets, a class-of-service (CoS) level for packet handling. Specify a value from 0 through 7:

- 1 or 2—Background. Packets are queued in AP forwarding queue 4.
- 0 or 3—Best effort. Packets are queued in AP forwarding queue 3.
- 4 or 5—Video. Packets are queued in AP forwarding queue 2. Use CoS level 4 or 5 for voice over IP (VoIP) packets other than SpectraLink Voice Priority (SVP).
- 6 or 7—Voice. Packets are queued in AP forwarding queue 1. Use 6 or 7 only for VoIP phones that use SVP, not for other types of traffic.

**deny** Blocks traffic that matches the conditions in the ACE.

*protocol* IP protocol by which to filter packets:

- ip
- tcp
- udp
- icmp
- A protocol number between 0 and 255


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| *source-ip-addr mask* **\| any** | IP address and wildcard mask of the network or host from which the packet is being sent. Specify both address and mask in dotted decimal notation. To match on any address, specify any or 0.0.0.0 255.255.255.255. |
| **operator** *port* [*port2*] | Operand and port number(s) for matching TCP or UDP packets to the number of the source or destination port on source-ip-addr or destination-ip-addr. Specify one of the following operands and the associated port:<br>• eq—Packets are filtered for only port number.<br>• gt—Packets are filtered for all ports that are greater than port number.<br>• lt—Packets are filtered for all ports that are less than port number.<br>• neq—Packets are filtered for all ports except port number.<br>• range—Packets are filtered for ports in the range between port and port2. To specify a port range, enter two port numbers. Enter the lower port number first, followed by the higher port number. |
| *destination-ip-addr mask* \| **any** | IP address and wildcard mask of the network or host to which the packet is being sent. Specify both address and mask in dotted decimal notation. To match on any address, specify any or 0.0.0.0 255.255.255.255. |
| **type** *icmp-type* | Filters ICMP messages by type. Specify a value from through 255. |
| **code** *icmp-code* | For ICMP messages filtered by type, additionally filters ICMP messages by code. Specify a value from 0 through 255. (For a list of ICMP message type and code numbers, see www.iana.org/assignments/icmp-parameters.) |
| **precedence** *precedence* | Filters packets by precedence level. Specify a value from 0 through 7:<br>• 0—routine precedence<br>• 1—priority precedence<br>• 2—immediate precedence<br>• 3—flash precedence<br>• 4—flash override precedence<br>• 5—critical precedence<br>• 6—internetwork control precedence<br>• 7—network control precedence |
| **tos** *tos* | Filters packets by type of service (TOS) level. Specify one of the following values, or any sum of these values up to 15. For example, a tos value of 9 filters packets with the TOS levels minimum delay (8) and minimum monetary cost (1).<br>• 8—minimum delay<br>• 4—maximum throughput<br>• 2—maximum reliability<br>• 1—minimum monetary cost<br>• 0—normal |


Download from Www.Somanuals.com. All Manuals Search And Download.

| | |
|---|---|
| **dscp** *codepoint* | Filters packets by Differentiated Services Code Point (DSCP) value. You can specify a number from 0 to 63, in decimal or binary format.<br><br>Note: You cannot use the dscp option along with the precedence and tos options in the same ACE. The CLI rejects an ACE that has this combination of options. |
| **established** | For TCP packets only, applies the ACE only to established TCP sessions and not to new TCP sessions. |
| **before** *editbuffer-index* | Inserts the new ACE in front of another ACE in the security ACL. Specify the number of the existing ACE in the edit buffer. Index numbers start at 1. (To display the edit buffer, use show security acl editbuffer.) |
| **modify** *editbuffer-index* | Replaces an ACE in the security ACL with the new ACE. Specify the number of the existing ACE in the edit buffer. Index numbers start at 1. (To display the edit buffer, use show security acl editbuffer.) |
| **hits** | Tracks the number of packets that are filtered based on a security ACL, for all mappings. |

**Defaults:** By default, permitted packets are classified based on DSCP value, which is converted into an internal CoS value in the switch's CoS map. The packet is then marked with a DSCP value based on the internal CoS value. If the ACE contains the cos option, this option overrides the switch's CoS map and marks the packet based on the ACE.

**Access:** Enabled.

**Usage:** The switch does not apply security ACLs until you activate them with the commit security acl command and map them to a VLAN, port, or virtual port, or to a user. If the switch is reset or restarted, any ACLs in the edit buffer are lost.

You cannot perform ACL functions that include permitting, denying, or marking with a Class of Service (CoS) level on packets with a multicast or broadcast destination address.

The order of security ACEs in a security ACL is important. Once an ACL is active, its ACEs are checked according to their order in the ACL. If an ACE criterion is met, its action takes place and any ACEs that follow are ignored. ACEs are listed in the order in which you create them, unless you move them. To position security ACEs within a security ACL, use before editbuffer-index and modify editbuffer-index.

**Examples:** The following command adds an ACE to security acl_123 that permits packets from IP address 192.168.1.11/24 and counts the hits:

```
DWS-1008# set security acl ip acl_123 permit 192.168.1.11 0.0.0.255 hits
```

The following command adds an ACE to acl_123 that denies packets from IP address 192.168.2.11:

```
DWS-1008# set security acl ip acl_123 deny 192.168.2.11 0.0.0.0
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The following command creates acl_125 by defining an ACE that denies TCP packets from source IP address 192.168.0.1 to destination IP address 192.168.0.2 for established sessions only, and counts the hits:

DWS-1008# **set security acl ip acl_125 deny tcp 192.168.0.1 0.0.0.0 192.168.0.2** 0.0.0.0 established hits

The following command adds an ACE to acl_125 that denies TCP packets from source IP address 192.168.1.1 to destination IP address 192.168.1.2, on destination port 80 only, and counts the hits:

DWS-1008# **set security acl ip acl_125 deny tcp 192.168.1.1 0.0.0.0 192.168.1.2** 0.0.0.0 eq 80 hits

Finally, the following command commits the security ACLs in the edit buffer to the configuration:

DWS-1008# **commit security acl all**
configuration accepted

**See Also:**
- clear security acl
- commit security acl
- show security acl

# set security acl map

Assigns a committed security ACL to a VLAN, physical port or ports, virtual port, or Distributed AP on the switch.

**Note:** To assign a security ACL to a user or group in the local database, use the command set user attr, set mac-user attr, set usergroup attr, or set mac-usergroup attr with the Filter-Id attribute. To assign a security ACL to a user or group with Filter-Id on a RADIUS server, see the documentation for your RADIUS server.

**Syntax: set security acl map** *acl-name* **{vlan** *vlan-id* **| port** *port-list* **[tag** *tag-list***] | dap** *dap-num***} {in | out}**

| | |
|---|---|
| *acl-name* | Name of an existing security ACL to map. ACL names start with a letter and are case-insensitive. |
| **vlan** *vlan-id* | VLAN name or number. MSS assigns the security ACL to the specified VLAN. |
| **port** *port-list* | Port list. MSS assigns the security ACL to the specified physical switch port or ports. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**tag** *tag-list* — One or more values that identify a virtual port in a VLAN. Specify a single tag value from 1 through 4095. Or specify a comma-separated list of values, a hyphen-separated range, or any combination, with no spaces. MSS assigns the security ACL to the specified virtual port or ports.

**dap** *dap-num* — One or more Distributed APs, based on their connection IDs. Specify a single connection ID, or specify a comma-separated list of connection IDs, a hyphen-separated range, or any combination, with no spaces. MSS assigns the security ACL to the specified Distributed APs.

**in** — Assigns the security ACL to traffic coming into the switch.

**out** — Assigns the security ACL to traffic coming from the switch.

**Defaults:** None.

**Access:** Enabled.

**Usage:** Before you can map a security ACL, you must use the commit security acl command to save the ACL in the running configuration and nonvolatile storage.

For best results, map only one input security ACL and one output security ACL to each VLAN, physical port, virtual port, or Distributed AP to filter a flow of packets. If more than one security ACL filters the same traffic, MSS applies only the first ACL match and ignores any other matches.

**Examples:** The following command maps security ACL acl_133 to port 4 for incoming packets:

```
DWS-1008 set security acl map acl_133 port 4 in
success: change accepted.
```

**See Also:**
- clear security acl map
- commit security acl
- set mac-user attr
- set mac-usergroup attr
- set security acl
- set user attr
- set usergroup
- show security acl map


Download from Www.Somanuals.com. All Manuals Search And Download.

# set security acl hit-sample-rate

Specifies the time interval, in seconds, at which the packet counter for each security ACL is sampled for display. The counter counts the number of packets filtered by the security ACL—or "hits."

**Syntax: set security acl hit-sample-rate** *seconds*

*seconds* Number of seconds between samples. A sample rate of 0 (zero) disables the sample process.

**Defaults:** By default, the hits are not sampled.

**Access:** Enabled.

**Usage:** To view counter results for a particular ACL, use the **show security acl info acl-name** command. To view the hits for all security ACLs, use the **show security acl hits** command.

**Examples:** The first command sets MSS to sample ACL hits every 15 seconds. The second and third commands display the results. The results show that 916 packets matching security acl_153 were sent since the ACL was mapped.

```
DWS-1008# set security acl hit-sample-rate 15

DWS-1008# show security acl info acl_153
ACL information for acl_153
set security acl ip acl_153 (hits #3 916)
-------------------------------------------------------
1. permit IP source IP 20.1.1.1 0.0.0.0 destination IP any enable-hits

DWS-1008# show security acl hits
ACL hit counters
Index  Counter      ACL-name
---------------------------------------
1      0            acl_2
2      0            acl_175
3      916          acl_153
```

**See Also:**
- show security acl hits
- show security acl info


Download from Www.Somanuals.com. All Manuals Search And Download.

# show security acl

Displays a summary of the security ACLs that are mapped.

**Syntax: show security acl**

**Defaults:** None.

**Access:** Enabled.

**Usage:** This command lists only the ACLs that have been mapped to something (a user, or VLAN, or port, and so on). To list all committed ACLs, use the **show security acl info** command. To list ACLs that have not yet been committed, use the **show security acl editbuffer** command.

**Examples:** To display a summary of the mapped security ACLs on a DWS-1008 switch, type the following command:

```
DWS-1008# show security acl
ACL table
ACL           Type   Class          Mapping
-------------------------------------------------------------
acl_123       IP     Static         Port 2 In
acl_133       IP     Static         Port 4 In
acl_124       IP     Static
```

**See Also:**
- clear security acl
- commit security acl
- set security acl
- show security acl editbuffer
- show security acl info


Download from Www.Somanuals.com. All Manuals Search And Download.

# show security acl editbuffer

Displays a summary of the security ACLs that have not yet been committed to the configuration.

**Syntax: show security acl [info all] editbuffer**

**info all** Displays the ACEs in each uncommitted ACL. Without this option, only the ACE names are listed.

**Defaults:** None.

**Access:** Enabled.

**Examples:** To view a summary of the security ACLs in the edit buffer, type the following command:

```
DWS-1008# show security acl editbuffer
ACL edit-buffer table
ACL Type Status
--------------------------- ---- --------------
acl_111 IP Not committed
acl-a IP Not committed
To view details about these uncommitted ACLs, type the following command.

DWS-1008# show security acl info all editbuffer
ACL edit-buffer information for all
set security acl ip acl-111 (ACEs 3, add 3, del 0, modified 2)
---------------------------------------------------
1. permit IP source IP 192.168.254.12 0.0.0.0 destination IP any
2. permit IP source IP 192.168.253.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.253.1 0.0.0.255
set security acl ip acl-a (ACEs 1, add 1, del 0, modified 0)
---------------------------------------------------
1. permit SRC source IP 192.168.1.1 0.0.0.0
```

**See Also:**

- clear security acl
- commit security acl
- set security acl
- show security acl
- show security acl info



Download from Www.Somanuals.com. All Manuals Search And Download.

# show security acl hits

Displays the number of packets filtered by security ACLs (“hits”) on the switch. Each time a packet is filtered by a security ACL, the hit counter increments.

**Syntax: show security acl hits**

**Defaults:** None.

**Access:** Enabled.

**Usage:** For MSS to count hits for a security ACL, you must specify hits in the set security acl commands that define ACE rules for the ACL.

**Examples:** To display the security ACL hits on a switch, type the following command:

```
DWS-1008# show security acl hits
ACL hit-counters
Index   Counter       ACL-name
-----------------------------------------
1       0             acl_2
2       0             acl_175
3       916           acl_123
```

**See Also:**
- hit-sample-rate
- set security acl

# show security acl info

Displays the contents of a specified security ACL or all security ACLs that are committed—saved in the running configuration and nonvolatile storage—or the contents of security ACLs in the edit buffer before they are committed.

**Syntax: show security acl info [*acl-nam*e | all] [editbuffer]**

| | |
|---|---|
| *acl-name* | Name of an existing security ACL to display. ACL names must start with a letter and are case-insensitive. |
| **all** | Displays the contents of all security ACLs. |
| **editbuffer** | Displays the contents of the specified security ACL or all security ACLs that are stored in the edit buffer after being created with set security acl. If you do not use this parameter, only committed ACLs are shown. |


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** Enabled.

**Examples:** To display the contents of all security ACLs committed on a switch, type the following command:

```
DWS-1008# show security acl info
ACL information for all
set security acl ip acl_123 (hits #5 462)
---------------------------------------------------------
1. permit IP source IP 192.168.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 192.168.2.11 0.0.0.0 destination IP any set security acl ip acl_134
(hits #3 0)
---------------------------------------------------------
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
---------------------------------------------------------
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
```

The following command displays the contents of acl_123 in the edit buffer, including the committed ACE rules 1 and 2 and the uncommitted rule 3:

```
DWS-1008# show security acl info acl_123 editbuffer
ACL edit-buffer information for acl_123
set security acl ip acl_123 (ACEs 3, add 3, del 0, modified 0)
---------------------------------------------------------
1. permit IP source IP 192.168.1.11 0.0.0.255 destination IP any
enable-hits
2. deny IP source IP 192.168.2.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.1.234 255.255.255.255 enable-hits
```

**See Also:**
- clear security acl
- commit security acl
- set security acl


Download from Www.Somanuals.com. All Manuals Search And Download.

# show security acl map

Displays the VLANs, ports, and virtual ports on the switch to which a security ACL is assigned.

**Syntax: show security acl map** *acl-name*

| | |
|---|---|
| *acl-name* | Name of an existing security ACL for which to show static mapping. ACL names must start with a letter and are case-insensitive. |

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command displays the port to which security ACL acl_111 is mapped:

```
DWS-1008# show security acl map acl_111
ACL acl_111 is mapped to:
Port 4 in
```

**See Also:**
- clear security acl map
- set security acl map
- show security acl

# show security acl resource-usage

Displays statistics about the resources used by security ACL filtering on the switch.

**Syntax: show security acl resource-usage**

**Defaults:** None.

**Access:** Enabled.

**Usage:** Use this command with the help of D-Link Technical Support to diagnose an ACL resource problem.


Download from Www.Somanuals.com. All Manuals Search And Download.

Examples To display security ACL resource usage, type the following command:

```
DWS-1008# show security acl resource-usage
ACL resources
Classifier tree counters
------------------------------
Number of rules:                2
Number of leaf nodes:           1
Stored rule count:              2
Leaf chain count:               1
Longest leaf chain:             2
Number of non-leaf nodes:       0
Uncompressed Rule Count:        2
Maximum node depth:             1
Sub-chain count:                0
PSCBs in primary memory:        0 (max: 512)
PSCBs in secondary memory:      0 (max: 9728)
Leaves in primary:              2 (max: 151)
Leaves in secondary:            0 (max 12096)
Sum node depth:                 1

Information on Network Processor status
-----------------------------------------------------
Fragmentation control :         0
UC switchdest :                 0
ACL resources
Port number :                   0
Number of action types :        2
LUdef in use :                  5
Default action pointer :        c8007dc
L4 global :                     True
No rules :                      False
Non-IP rules :                  False
Root in first :                 True
Static default action :         False
No per-user (MAC) mapping :     True
Out mapping :                   False
In mapping :                    True
No VLAN or PORT mapping :       False
No VPORT mapping :              True
```

The table on the next page explains the fields in the **show security acl resource-usage** output.


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| Number of rules | Number of security ACEs currently mapped to ports or VLANs. |
| Number of leaf nodes | Number of security ACL data entries stored in the rule tree. |
| Stored rule count | Number of security ACEs stored in the rule tree. |
| Leaf chain count | Number of chained security ACL data entries stored in the rule tree. |
| Longest leaf chain | Longest chain of security ACL data entries stored in the rule tree. |
| Number of non-leaf nodes | Number of nodes with no data entries stored in the rule tree. |
| Uncompressed Rule Count | Number of security ACEs stored in the rule tree, including duplicates—ACEs in ACLs applied to multiple ports, virtual ports, or VLANs. |
| Maximum node depth | Number of data elements in the rule tree, from the root to the furthest data entry (leaf). |
| Sub-chain count | Sum of action types represented in all security ACL data entries. |
| PSCBs in primary memory | Number of pattern search control blocks (PSCBs) stored in primary node memory. |
| PSCBs in secondary memory | Number of PSCBs stored in secondary node memory. |
| Leaves in primary | Number of security ACL data entries stored in primary leaf memory. |
| Leaves in secondary | Number of ACL data entries stored in secondary leaf memory. |
| Sum node depth | Total number of security ACL data entries. |
| Fragmentation control | Control value for handling fragmented IP packets.<br>**Note:** The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments. |
| UC switchdest | Control value for handling fragmented IP packets.<br>**Note:** The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments. |
| Port number | Control value for handling fragmented IP packets.<br>**Note:** The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments. |
| Number of action types | Number of actions that can be performed by ACLs. This value is always 2, because ACLs can either permit or deny. |
| LUdef in use | Number of the lookup definition (LUdef) table currently in use for packet handling. |
| Default action pointer | Memory address used for packet handling, from which default action data is obtained when necessary. |
| L4 global | Security ACL mapping on the switch:<br>• True—Security ACLs are mapped.<br>• False—No security ACLs are mapped. |
| No rules | Security ACE rule mapping on the switch:<br>• True—No security ACEs are mapped.<br>• False—Security ACEs are mapped. |
| Non-IP rules | Non-IP security ACE mapping on the switch:<br>• True—Non-IP security ACEs are mapped.<br>• False—Only IP security ACEs are mapped.<br>Note: The current MSS version supports security ACEs for IP only. |
| Root in first | Leaf buffer allocation:<br>• True - Enough primary leaf buffers are allocated in nonvolatile memory to accommodate all leaves.<br>• False - Insufficient primary leaf buffers are allocated in nonvolatile memory to accommodate all leaves. |


Download from Www.Somanuals.com. All Manuals Search And Download.

| Field | Description |
|---|---|
| Static default action | Definition of a default action:<br>• True—A default action types is defined.<br>• False—No default action type is defined. |
| No per-user (MAC) mapping | Per-user application of a security ACL with the Filter-Id attribute, on the switch:<br>• True—No security ACLs are applied to users.<br>• False—Security ACLs are applied to users. |
| Out mapping | Application of security ACLs to outgoing traffic on the switch:<br>• True—Security ACLs are mapped to outgoing traffic.<br>• False—No security ACLs are mapped to outgoing traffic. |
| In mapping | Application of security ACLs to incoming traffic on the switch:<br>• True—Security ACLs are mapped to incoming traffic.<br>• False—No security ACLs are mapped to incoming traffic. |
| No VLAN or PORT mapping | Application of security ACLs to VLANs or ports on the switch:<br>• True—No security ACLs are mapped to VLANs or ports.<br>• False—Security ACLs are mapped to VLANs or ports. |
| No VPORT mapping | Application of security ACLs to virtual ports on the switch:<br>• True—No security ACLs are mapped to virtual ports.<br>• False—Security ACLs are mapped to virtual ports. |
| Packets with bad IGMP checksum | Number of packets with an invalid IGMP checksum value. |
| Packets dropped | Number of multicast packets dropped by the switch. |


Download from Www.Somanuals.com. All Manuals Search And Download.

# Trace Commands

Use trace commands to perform diagnostic routines. While MSS allows you to run many types of traces, this chapter describes commands for those traces you are most likely to use. For a complete listing of the types of traces MSS allows, type the **set trace ?** command.

**Caution:** Using the **set trace command** can have adverse effects on system performance. D-Link recommends that you use the lowest levels possible for initial trace commands, and slowly increase the levels to get the data you need.

This chapter presents trace commands alphabetically. Use the following table to locate commands in this chapter based on their use.


**Trace**

clear log trace on page 490
clear trace on page 491
save trace on page 492
set trace authentication on page 492
set trace authorization on page 493
set trace dot1x on page 493
set trace sm on page 494
show trace on page 495


## clear log trace

Deletes the log messages stored in the trace buffer.

**Syntax: clear log trace**

**Defaults:** None.

**Access:** Enabled.

**Examples:** To delete the trace log, type the following command:

```
DWS-1008# clear log trace
```

**See Also:**
- set log
- show log buffer


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear trace

Deletes running trace commands and ends trace processes.

**Syntax: clear trace {***trace-area* **| all}**

*trace-area* Ends a particular trace process. Specify one of the following keywords to end the traces documented in this chapter:

- **authorization**—Ends an authorization trace
- **dot1x**—Ends an 802.1X trace
- **authentication**—Ends an authentication trace
- **sm**—Ends a session manager trace all Ends all trace processes.

**Defaults:** None.

**Access:** Enabled.

**Examples:** To clear all trace processes, type the following command:

```
DWS-1008# clear trace all
success: clear trace all
```

To clear the session manager trace, type the following command:

```
DWS-1008# clear trace sm
success: clear trace sm
```

**See Also:**
- set trace authentication
- set trace authorization
- set trace dot1x
- set trace sm
- show trace


Download from Www.Somanuals.com. All Manuals Search And Download.

# save trace

Saves the accumulated trace data for enabled traces to a file in the switch's nonvolatile storage.

**Syntax: save trace** *filename*

*filename* Name for the trace file. To save the file in a subdirectory, specify the subdirectory name, then a slash. For example: **traces/trace1**

**Defaults:** None.

**Access:** Enabled.

**Examples:** To save trace data into the file trace1 in the subdirectory traces, type the following command:

```
DWS-1008# save trace traces/trace1
```

# set trace authentication

Traces authentication information.

**Syntax: set trace authentication [mac-addr** *mac-address***] [port** *port-num***] [user** *username***] [level** *level***]**

**mac-addr** *mac-address* Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).

**port** *port-num* Traces a port number. Specify a port number between 1 and 22.

**user** *username* Traces a user. Specify a username of up to 32 alphanumeric characters with no spaces.

**level** *level* Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

**Defaults:** The default trace level is 5.

**Access:** Enabled.

**Examples:** The following command starts a trace for information about user jose's authentication:

```
DWS-1008# set trace authentication user jose
success: change accepted.
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# set trace authorization

Traces authorization information.

**Syntax: set trace authorization [mac-addr** *mac-address***] [port** *port-num***] [user** *username***] [level** *level***]**

**mac-addr** *mac-address* Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).

**port** *port-num* Traces a port number. Specify a port number between 1 and 22.

**user** *username* Traces a user. Specify a username of up to 80 alphanumeric characters with no spaces.

**level** *level* Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

**Defaults:** The default trace level is 5.

**Access:** Enabled.

**Examples:** The following command starts a trace for information for authorization for MAC address 00:01:02:03:04:05:

```
DWS-1008# set trace authorization mac-addr 00:01:02:03:04:05
success: change accepted.
```

**See Also:**
- clear trace
- show trace

# set trace dot1x

Traces 802.1X sessions.

**Syntax: set trace dot1x [mac-addr** *mac-address***] [port** *port-num***] [user** *username***] [level** *level***]**

**mac-addr** *mac-address* Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).


Download from Www.Somanuals.com. All Manuals Search And Download.

**port** *port-num* — Traces a port number. Specify a port number between 1 and 22.

**user** *username* — Traces a user. Specify a username of up to 80 alphanumeric characters with no spaces.

**level** *level* — Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

**Defaults:** The default trace level is 5.

**Access:** Enabled.

**Examples:** The following command starts a trace for the 802.1X sessions for MAC address 00:01:02:03:04:05:

```
DWS-1008# set trace dot1x mac-addr 00:01:02:03:04:05:
success: change accepted.
```

**See Also:**
- clear trace
- show trace

# set trace sm

Traces session manager activity.

**Syntax: set trace sm [mac-addr** *mac-address***] [port** *port-num***] [user** *username***] [level** *level***]**

**mac-addr** *mac-address* — Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).

**port** *port-num* — Traces a port number. Specify a port number between 1 and 22.

**user** *username* — Traces a user. Specify a username of up to 80 alphanumeric characters, with no spaces.

**level** *level* — Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** The default trace level is 5.

**Access:** Enabled.

**Examples:** Type the following command to trace session manager activity for MAC address 00:01:02:03:04:05:

```
DWS-1008# set trace sm mac-addr 00:01:02:03:04:05:
success: change accepted.
```

**See Also:**
- clear trace
- show trace

# show trace

Displays information about traces that are currently configured on the switch, or all possible trace options.

**Syntax: show trace [all]**

**all** Displays all possible trace options and their configuration.

**Defaults:** None.

**Access:** Enabled.

**Examples:** To view the traces currently running, type the following command:

```
DWS-1008# show trace
milliseconds spent printing traces: 1885.614
Trace Area          Level Mac          User                Port Filter
-------------------------------------------------------------------------------------
dot1x               5                                      0
sm                  5                                      0
```

**See Also:**
- clear trace
- set trace authentication
- set trace authorization
- set trace dot1x
- set trace sm


Download from Www.Somanuals.com. All Manuals Search And Download.

# Snoop Commands

Use snoop commands to monitor wireless traffic, by using a Distributed AP as a sniffing device. The AP copies the sniffed 802.11 packets and sends the copies to an observer, which is typically a protocol analyzer such as Ethereal or Tethereal.

This chapter presents snoop commands alphabetically. Use the following table to locate commands in this chapter based on their use.


**Remote monitoring (snooping)**

clear snoop on page 496
clear snoop map on page 497
set snoop on page 497
set snoop map on page 500
set snoop mode on page 501
show snoop on page 502
show snoop info on page 502
show snoop map on page 503
show snoop stats on page 503


## clear snoop

Deletes a snoop filter.

**Syntax: clear snoop** *filter-name*

*filter-name* Name of the snoop filter.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command deletes snoop filter snoop1:

```
DWS-1008# clear snoop snoop1
```

**See Also:**
- set snoop
- show snoop info


Download from Www.Somanuals.com. All Manuals Search And Download.

# clear snoop map

Removes a snoop filter from an AP radio.

**Examples: clear snoop map** *filter-name* **dap** *dap-num* **radio {1 | 2}**

*filter-name* Name of the snoop filter.

**dap** *dap-num* Number of a Distributed AP to which to snoop filter is mapped.

**radio 1** Radio 1 of the AP.

**radio 2** Radio 2 of the AP. (This option does not apply to single-radio models.)

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command removes snoop filter snoop2 from radio 2 on Distributed AP 3:

```
DWS-1008# clear snoop map snoop2 dap 3 radio 2
success: change accepted.
```

The following command removes all snoop filter mappings from all radios:

```
DWS-1008# clear snoop map all
success: change accepted.
```

**See Also:**
- set snoop map
- show snoop
- show snoop map

# set snoop

Configures a snoop filter.

**Syntax: set snoop** *filter-name* **[***condition-list***] [observer** *ip-addr***] [snap-length** *num***]**

*filter-name* Name for the filter. The name can be up to 15 alphanumeric characters, with no spaces.


Download from Www.Somanuals.com. All Manuals Search And Download.

*condition-list* — Match criteria for packets. Conditions in the list are ANDed. Therefore, to be copied and sent to an observer, a packet must match all criteria in the *condition-list*. You can specify up to eight of the following conditions in a filter, in any order or combination:

- **frame-type {eq | neq} {beacon | control | data | management | probe}**
- **channel {eq | neq}** *channel*
- **bssid {eq | neq}** *bssid*
- **src-mac {eq | neq | lt | gt}** *mac-addr*
- **dest-mac {eq | neq | lt | gt}** *mac-addr*
- **host-mac {eq | neq | lt | gt}** *mac-addr*
- **mac-pair** *mac-addr1 mac-addr2*

To match on packets to or from a specific MAC address, use the **dest-mac** or **src-mac** option. To match on both send and receive traffic for a host address, use the **host-mac** option.

To match on a traffic flow (source and destination MAC addresses), use the **mac-pair** option. This option matches for either direction of a flow, and either MAC address can be the source or destination address.

If you omit a condition, all packets match that condition. For example, if you omit frame-type, all frame types match the filter.

For most conditions, you can use **eq** (equal) to match only on traffic that matches the condition value. Use **neq** (not equal) to match only on traffic that is not equal to the condition value.

The **src-mac**, **dest-mac**, and **host-mac** conditions also support lt (less than) and gt (greater than).

**observer** *ip-addr* — Specifies the IP address of the station where the protocol analyzer is located. If you do not specify an observer, the AP radio still counts the packets that match the filter.

**snap-length** *num* — Specifies the maximum number of bytes to capture. If you do not specify a length, the entire packet is copied and sent to the observer. D-Link recommends specifying a snap length of 100 bytes or less.

**Defaults:** No snoop filters are configured by default.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

Usage Traffic that matches a snoop filter is copied after it is decrypted. The decrypted (clear) version is sent to the observer.

For best results:

- Do not specify an observer that is associated with the AP where the snoop filter is running. This configuration causes an endless cycle of snoop traffic.

- If the snoop filter is running on a Distributed AP, and the AP used a DHCP server in its local subnet to configure its IP information, and the AP did not receive a default router (gateway) address as a result, the observer must also be in the same subnet. Without a default router, the AP cannot find the observer.

- The AP that is running a snoop filter forwards snooped packets directly to the observer. This is a one-way communication, from the AP to the observer. If the observer is not present, the AP still sends the snoop packets, which use bandwidth. If the observer is present but is not listening to TZSP traffic, the observer continuously sends ICMP error indications back to the AP. These ICMP messages can affect network and AP performance.

**Examples:** The following command configures a snoop filter named snoop1 that matches on all traffic, and copies the traffic to the device that has IP address 10.10.30.2:

```
DWS-1008# set snoop snoop1 observer 10.10.30.2 snap-length 100
```

The following command configures a snoop filter named snoop2 that matches on all data traffic between the device with MAC address aa:bb:cc:dd:ee:ff and the device with MAC address 11:22:33:44:55:66, and copies the traffic to the device that has IP address 10.10.30.3:

```
DWS-1008# set snoop snoop2 frame-type eq data mac-pair aa:bb:cc:dd:ee:ff
11:22:33:44:55:66 observer 10.10.30.3 snap-length 100
```

**See Also:**
- clear snoop
- set snoop map
- set snoop mode
- show snoop info
- show snoop stats


Download from Www.Somanuals.com. All Manuals Search And Download.

# set snoop map

Maps a snoop filter to a radio on a Distributed AP. A snoop filter does take effect until you map it to a radio and enable the filter.

**Examples: set snoop map** *filter-name* **dap** *dap-num* **radio {1 | 2}**

| | |
|---|---|
| *filter-name* | Name of the snoop filter. |
| **dap** *dap-num* | Number of a Distributed AP to which to map the snoop filter. |
| **radio 1** | Radio 1 of the AP. |
| **radio 2** | Radio 2 of the AP. (This option does not apply to single-radio models.) |

**Defaults:** Snoop filters are unmapped by default.

**Access:** Enabled.

**Usage:** You can map the same filter to more than one radio. You can map up to eight filters to the same radio. If more than one filter has the same observer, the AP sends only one copy of a packet that matches a filter to the observer. After the first match, the AP sends the packet and stops comparing the packet against other filters for the same observer.

If the filter does not have an observer, the AP still maintains a counter of the number of packets that match the filter.

**Examples:** The following command maps snoop filter snoop1 to radio 2 on Distributed AP 3:

```
DWS-1008# set snoop map snoop1 dap 3 radio 2
success: change accepted.
```

**See Also:**
- clear snoop map
- set snoop
- set snoop mode
- show snoop map
- show snoop stats


Download from Www.Somanuals.com. All Manuals Search And Download.

# set snoop mode

Enables a snoop filter. A snoop filter does not take effect until you map it to an AP radio and enable the filter.

**Examples: set snoop {***filter-name* **| all}**
**mode {enable [stop-after** *num-pkts***] | disable}**

| | |
|---|---|
| {filter-name \| **all**} | Name of the snoop filter. Specify all to enable all snoop filters. |
| **enable [stop-after** *num-pkts*] | Enables the snoop filter. The **stop-after** option disables the filter after the specified number of packets match the filter. Without the **stop-after** option, the filter operates until you disable it or until the AP is restarted. |
| **disable** | Disables the snoop filter. |

**Defaults:** Snoop filters are disabled by default.

**Access:** Enabled.

**Usage:** The filter mode is not retained if you change the filter configuration or disable and reenable the radio, or when the AP or the switch is restarted. You must reenable the filter to place it back into effect.

**Examples:** The following command enables snoop filter snoop1, and configures the filter to stop after 5000 packets match the filter:

```
DWS-1008# set snoop snoop1 mode enable stop-after 5000
success: filter 'snoop1' enabled
```

**See Also:**
- show snoop
- show snoop info
- show snoop map
- show snoop stats


Download from Www.Somanuals.com. All Manuals Search And Download.

# show snoop

Displays the AP radio mapping for all snoop filters.

**Syntax: show snoop**

**Defaults:** None.

**Access:** Enabled.

**Usage:** To display the mappings for a specific AP radio, use the **show snoop map** command.

**Examples:** The following command shows the AP radio mappings for all snoop filters configured on a DWS-1008 switch:

```
DWS-1008# show snoop
Dap: 3 Radio: 2
snoop1
snoop2
Dap: 2 Radio: 2
snoop2
```

**See Also:**
- clear snoop map
- set snoop map
- show snoop map

# show snoop info

Shows the configured snoop filters.

**Syntax: show snoop** *filter-name*

*filter-name* Name of the snoop filter.

**Defaults:** None.

**Access:** Enabled.

**Examples:** The following command shows the snoop filters configured in the examples above:

```
DWS-1008# show snoop info
snoop1:
        observer 10.10.30.2 snap-length 100
        all packets
snoop2:
        observer 10.10.30.3 snap-length 100
        frame-type eq data
        mac-pair (aa:bb:cc:dd:ee:ff, 11:22:33:44:55:66)
```

**See Also:**
- clear snoop
- set snoop


Download from Www.Somanuals.com. All Manuals Search And Download.

# show snoop map

Shows the AP radios that are mapped to a specific snoop filter.

**Syntax: show snoop map** *filter-name*

*filter-name* Name of the snoop filter.

**Defaults:** None.

**Access:** Enabled.

**Usage:** To display the mappings for all snoop filters, use the show snoop command.

**Examples:** The following command shows the mapping for snoop filter snoop1:

```
DWS-1008# show snoop map snoop1
filter 'snoop1' mapping
Dap: 3 Radio: 2
```

**See Also:**
- clear snoop map
- set snoop map
- show snoop

# show snoop stats

Displays statistics for enabled snoop filters.

**Examples: show snoop stats [***filter-name* **[***dap-num* **[radio {1 | 2}]]]**

*filter-name* Name of the snoop filter.

**dap** *dap-num* Number of a Distributed AP to which the snoop filter is mapped.

**radio 1** Radio 1 of the AP.

**radio 2** Radio 2 of the AP. (This option does not apply to single-radio models.)

**Defaults:** None.

**Access:** Enabled.

**Usage:** The AP retains statistics for a snoop filter until the filter is changed or disabled. The AP then clears the statistics.

**Examples:** The following command shows statistics for snoop filter snoop1:

```
DWS-1008# show snoop stats snoop1
Filter          Dap   Radio Rx Match     Tx Match     Dropped     Stop-After
=============================================================
snoop1          3     1     96           4            0           stopped
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields in this display.

| Field | Description |
|---|---|
| Filter | Name of the snoop filter. |
| Dap | Distributed AP containing the radio to which the filter is mapped. |
| Radio | Radio to which the filter is mapped. |
| Rx Match | Number of packets received by the radio that match the filter. |
| Tx Match | Number of packets sent by the radio that match the filter. |
| Dropped | Number of packets that matched the filter but that were not copied to the observer due to memory or network problems. |
| Stop-After | Filter state:<br>• running—enabled<br>• stopped—disabled<br>• number-of-packets—If the filter is running and the stop-after option was used to stop the filter, this field displays the number of packets that still need to match before the filter is stopped. |


Download from Www.Somanuals.com. All Manuals Search And Download.

# System Log Commands

Use the system log commands to record information for monitoring and troubleshooting. MSS system logs are based on RFC 3164, which defines the log protocol.

This chapter presents system log commands alphabetically. Use the following table to locate commands in this chapter based on their use.


**System Logs**

clear log on page 505
set log on page 506
set log mark on page 508
show log buffer on page 509
show log config on page 510
show log trace on page 511


## clear log

Clears the log messages stored in the log buffer, or removes the configuration for a syslog server and stops sending log messages to that server.

**Syntax: clear log [buffer | server ip-addr]**

**buffer** Deletes the log messages stored in nonvolatile storage.

**server** *ip-addr* Deletes the configuration for and stops sending log messages to the syslog server at this IP address. Specify an address in dotted decimal notation.

**Defaults:** None.

**Access:** Enabled.

**Examples:** To stop sending system logging messages to a server at 192.168.253.11, type the following command:

```
DWS-1008# clear log server 192.168.253.11
success: change accepted.
```

Type the following command to clear all messages from the log buffer:

```
DWS-1008# clear log buffer
success: change accepted.
```

**See Also:**
- clear log trace
- set log



Download from Www.Somanuals.com. All Manuals Search And Download.

# set log

Enables or disables logging of DWS-1008 and AP events to the log buffer or other logging destination and sets the level of the events logged. For logging to a syslog server only, you can also set the facility logged.

**Syntax: set log {buffer | console | current | sessions | trace}**
**[severity** *severity-level***] [enable | disable]**

**set log server** *ip-addr* **[port** *port-number***] severity** *severity-level*
**[local-facility** *facility-level***]**

**buffer** — Sets log parameters for the log buffer in nonvolatile storage.

**console** — Sets log parameters for console sessions.

**current** — Sets log parameters for the current Telnet or console session. These settings are not stored in nonvolatile memory.

**server** *ip-addr* — Sets log parameters for a syslog server. Specify an address in dotted decimal notation.

**sessions** — Sets the default log values for Telnet sessions. You can set defaults for the following log parameters:

- Severity
- Logging state (enabled or disabled)

To override the session defaults for an individual session, type the **set log** command from within the session and use the current option.

**trace** — Sets log parameters for trace files.

**port** *port-number* — Sets the TCP port for sending messages to the syslog server. You can specify a number from 1 to 65535. The default syslog port is 514.

**severity** *severity-level* — Logs events at a severity level greater than or equal to the level specified. Specify one of the following:

- **emergency**—The switch is unusable.
- **alert**—Action must be taken immediately.
- **critical**—You must resolve the critical conditions. If the conditions are not resolved, the switch can reboot or shut down.
- **error**—The switch is missing data or is unable to form a connection.
- **warning**—A possible problem exists.
- **notice**—Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.
- **info**—Informational messages only. No problem exists.
- **debug**—Output from debugging.


Download from Www.Somanuals.com. All Manuals Search And Download.

**local-facility** *facility-level* For messages sent to a syslog server, maps all messages of the severity you specify to one of the standard local log facilities defined in RFC 3164. You can specify one of the following values:

- 0—maps all messages to local0.
- 1—maps all messages to local1.
- 2—maps all messages to local2.
- 3—maps all messages to local3.
- 4—maps all messages to local4.
- 5—maps all messages to local5.
- 6—maps all messages to local6.
- 7—maps all messages to local7.

If you do not specify a local facility, MSS sends the messages with their default MSS facilities. For example, AAA messages are sent with facility 4 and boot messages are sent with facility 20 by default.

**enable** Enables messages to the specified target.

**disable** Disables messages to the specified target.

**Defaults:**
- Events at the error level and higher are logged to the switch console.
- Events at the error level and higher are logged to the switch system buffer.
- Trace logging is enabled, and debug-level output is stored in the switch trace buffer.

**Access:** Enabled.

**Usage:** Using the command with only enable or disable turns logging on or off for the target at all levels. For example, entering set log buffer enable with no other keywords turns on logging to the system buffer of all facilities at all levels. Entering set log buffer disable with no other keywords turns off all logging to the buffer.

**Examples:** To log only emergency, alert, and critical system events to the console, type the following command:

```
DWS-1008# set log console severity critical enable
success: change accepted.
```

**See Also:**
- show log config
- clear log


Download from Www.Somanuals.com. All Manuals Search And Download.

# set log mark

Configures MSS to generate mark messages at regular intervals. The mark messages indicate the current system time and date. D-Link can use the mark messages to determine the approximate time when a system restart or other event causing a system outage occurred.

**Syntax: set log mark [enable | disable] [severity** *level***] [interval** *interval***]**

**enable** Enables the mark messages.

**disable** Disables the mark messages.

**severity** *level* Log severity at which the messages are logged:

- emergency
- alert
- critical
- error
- warning
- notice
- info
- debug

**interval** *interval* Interval at which MSS generates the mark messages. You can specify from 1 to 2147483647 seconds.

**Defaults:** Mark messages are disabled by default. When they are enabled, MSS generates a message at the notice level once every 300 seconds by default.

**Access:** Enabled.

**Examples:** The following command enables mark messages:

```
DWS-1008# set log mark enable
success: change accepted.
```

**See Also:**
- show log config


Download from Www.Somanuals.com. All Manuals Search And Download.

# show log buffer

Displays system information stored in the nonvolatile log buffer or the trace buffer.

**Syntax: show log buffer [{+/-}*number-of-messages*] [facility *facility-name*] [matching *string*] [severity *severity-level*]**

**buffer** Displays the log messages in nonvolatile storage.

*+/- number-of-messages* Displays the number of messages specified as follows:

- A positive number (for example, +100), displays that number of log entries starting from the oldest in the log.
- A negative number (for example, -100) displays that number of log entries starting from newest in the log.

**facility** *facility-name* Area of MSS that is sending the log message. Type a space and a question mark (?) after show log buffer facility for a list of valid facilities.

**matching** *string* Displays messages that match a string—for example, a username or IP address.

**severity** *severity-level* Displays messages at a severity level greater than or equal to the level specified. Specify one of the following:

- **emergency**—The switch is unusable.
- **alert**—Action must be taken immediately.
- **critical**—You must resolve the critical conditions. If the conditions are not resolved, the switch can reboot or shut down.
- **error**—The switch is missing data or is unable to form a connection.
- **warning**—A possible problem exists.
- **notice**—Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.
- **info**—Informational messages only. No problem exists.
- **debug**—Output from debugging.

**Defaults:** None.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Usage:** The debug level produces a lot of messages, many of which can appear to be somewhat cryptic. Debug messages are used primarily by D-Link for troubleshooting and are not intended for administrator use.

**Examples:** Type the following command to see the facilities for which you can view event messages archived in the buffer:

```
DWS-1008# show log buffer facility ?
<facility name> Select one of: KERNEL, AAA, SYSLOGD, ACL, APM,
ARP, ASO, BOOT, CLI, CLUSTER, CRYPTO, DOT1X, NET, ETHERNET, GATEWAY,
HTTPD, IGMP, IP, MISC, NOSE, NP, RAND, RESOLV, RIB, ROAM, ROGUE, SM,
SNMPD, SPAN, STORE, SYS, TAGMGR, TBRIDGE, TCPSSL, TELNET, TFTP, TLS,
TUNNEL, VLAN, X509, XML, AP, RAPDA, WEBVIEW, EAP, FP, STAT, SSHD,
SUP, DNSD, CONFIG, BACKUP.
```

The following command displays logged messages for the AAA facility:

```
DWS-1008# show log buffer facility AAA
AAA Jun. 25 09:11:32.579848 ERROR AAA_NOTIFY_ERR: AAA got SM special
event (98) on locality 3950 which is gone
```

**See Also:**
- clear log
- show log config

# show log config

Displays log configuration information.

**Syntax: show log config**

**Defaults:** None.

**Access:** Enabled.

**Examples:** To display how logging is configured, type the following command:

```
DWS-1008# show log config
Logging console: disabled
Logging console severity: DEBUG
Logging sessions: disabled
Logging sessions severity: INFO
Logging buffer: enabled
Logging buffer severity: WARNING
Logging trace: enabled
Logging trace severity: DEBUG
Logging buffer size: 10485760 bytes
Log marking: disabled
Log marking severity: NOTICE
Log marking interval: 300 seconds
Logging server: 172.21.12.19 port 514 severity EMERGENCY
Current session: disabled
Current session severity: INFO
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# show log trace

Displays system information stored in the nonvolatile log buffer or the trace buffer.

**Syntax: show log trace [{*+|-|/*} *number-of-messages*] [**facility** *facility-name*] [**matching** *string*] [**severity** *severity-level*]**

| | |
|---|---|
| **trace** | Displays the log messages in the trace buffer. |
| *+\|-\|/ number-of-messages* | Displays the number of messages specified as follows:<br>• A positive number (for example, +100), displays that number of log entries starting from the oldest in the log.<br>• A negative number (for example, -100) displays that number of log entries starting from newest in the log.<br>• A number preceded by a slash (for example, /100) displays that number of the most recent log entries in the log, starting with the least recent. |
| **facility** *facility-name* | Area of MSS that is sending the log message. Type a space and a question mark (?) after show log trace facility for a list of valid facilities. |
| **matching** *string* | Displays messages that match a string—for example, a username or IP address. |
| **severity** *severity-level* | Displays messages at a severity level greater than or equal to the level specified. Specify one of the following:<br>• **emergency**—The switch is unusable.<br>• **alert**—Action must be taken immediately.<br>• **critical**—You must resolve the critical conditions. If the conditions are not resolved, the switch can reboot or shut down.<br>• **error**—The switch is missing data or is unable to form a connection.<br>• **warning**—A possible problem exists.<br>• **notice**—Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.<br>• **info**—Informational messages only. No problem exists.<br>• **debug**—Output from debugging. |

**Defaults:** None.

**Access:** Enabled.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** Type the following command to see the facilities for which you can view event messages archived in the buffer:

```
DWS-1008# show log trace facility ?
<facility name> Select one of: KERNEL, AAA, SYSLOGD, ACL, APM,
ARP, ASO, BOOT, CLI, CLUSTER, CRYPTO, DOT1X, ENCAP, ETHERNET, GATEWAY,
HTTPD, IGMP, IP, MISC, NOSE, NP, RAND, RESOLV, RIB, ROAM, ROGUE, SM,
SNMPD, SPAN, STORE, SYS, TAGMGR, TBRIDGE, TCPSSL, TELNET, TFTP, TLS,
TUNNEL, VLAN, X509, XML, AP, RAPDA, WEBVIEW, EAP, PORTCONFIG, FP.
```

The following command displays the newest five trace log entries for the ROGUE facility:

```
DWS-1008# show log trace +5 facility ROGUE
ROGUE Oct 28 16:30:19.695141 ERROR ROGUE_AP_ALERT: Xmtr Mac
01:0b:0e:ff:00:3b Po
rt 7 Radio 1 Chan 36 RSSI 18 Tech DOT_11A SSID dlink
ROGUE Oct 28

16:30:19.7046
37 ERROR ROGUE_AP_ALERT: Xmtr Mac 01:0b:0e:00:09:5f Port 7 Radio 1 Chan
36 RSSI
15 Tech DOT_11A SSID examplewlan
ROGUE Oct 28 16:30:19.711253 ERROR
ROGUE_AP_ALER
T: Xmtr Mac 01:0b:0e:00:06:b7 Port 7 Radio 1 Chan 36 RSSI 36 Tech DOT_11A
SSID wlan-7
ROGUE Oct 28 16:30:19.717954 ERROR ROGUE_AP_ALERT: Xmtr Mac
00:0b:0e:00:0
6:8f Port 7 Radio 1 Chan 36 RSSI 13 Tech DOT_11A SSID trapeze
ROGUE Oct 28
16:30:
19.727069 ERROR ROGUE_AP_ALERT: Xmtr Mac 01:0b:0e:da:da:dd Port 7 Radio
1 Chan 3
6 RSSI 22 Tech DOT_11A SSID dlink
```

**See Also:**

- clear log
- show log config


Download from Www.Somanuals.com. All Manuals Search And Download.

# Boot Prompt Commands

Boot prompt commands enable you to perform basic tasks, including booting a system image file, from the boot prompt (boot>). A CLI session enters the boot prompt if MSS does not boot successfully or you intentionally interrupt the boot process. To interrupt the boot process, press **q** followed by Enter (return).

**Caution:** Generally, boot prompt commands are used only for troubleshooting. D-Link recommends that you use these commands only when working with D-Link to diagnose a system issue. In particular, commands that change boot parameters can interfere with a switch's ability to boot successfully.

This chapter presents boot prompt commands alphabetically. Use the following table to locate commands in this chapter based on their use.


| | |
|---|---|
| **Command Information** | help on page 521<br>ls on page 522 |
| **Booting** | autoboot on page 514<br>boot on page 514<br>dhcp on page 518<br>reset on page 524 |
| **File Management** | dir on page 519<br>fver on page 520<br>version on page 527 |
| **Boot Profile Management** | change on page 516<br>create on page 517<br>delete on page 518<br>next on page 523<br>show on page 525 |
| **Diagnostics** | diag on page 519<br>test on page 527 |




Download from Www.Somanuals.com. All Manuals Search And Download.

# autoboot

Displays or changes the state of the autoboot option. The autoboot option controls whether a DWS-1008 switch automatically boots a system image after initializing the hardware, following a system reset or power cycle.

**Syntax: autoboot [ON | on | OFF | off]**

**ON** Enables the autoboot option.

**on** Same effect as ON.

**OFF** Disables the autoboot option.

**off** Same effect as OFF.

**Defaults:** The autoboot option is enabled by default.

**Access:** Boot prompt.

**Examples:** The following command displays the current setting of the autoboot option:

```
boot> autoboot
The autoboot flag is on.
```

**See Also:**
• boot

# boot

Loads and executes a system image file.

**Syntax: boot [BT=*type*] [DEV=*device*] [FN=*filename*] [HA=*ip-addr*] [FL=*num*] [OPT=*option*] [OPT+=*option*]**

**BT**=*type* Boot type:
• c—Compact flash. Boots using nonvolatile storage or a flash card.
• n—Network. Boots using a TFTP server.

**DEV**=*device* Location of the system image file:
• c:—Nonvolatile storage area containing boot partition 0
• d:—Nonvolatile storage area containing boot partition 1
• e:—Primary partition of the flash card in the flash card slot
• f:—Secondary partition of the flash card in the flash card slot
• boot0—boot partition 0
• boot1—boot partition 1

When the boot type is n (network), the device can be one of the following:
• mgmt or tsec0—The 10/100 port labelled Mgmt

**FN**=*filename* System image filename.


Download from Www.Somanuals.com. All Manuals Search And Download.

**HA**=*ip-addr* Host address (IP address) of a TFTP server. This parameter applies only when the boot type is n (network).

**FL**=*num* Number representing the bit settings of boot flags to pass to the booted system image. Use this parameter only if advised to do so by D-Link.

**OPT**=*option* String up to 128 bytes of boot options to pass to the booted system image instead of the boot option(s) in the currently active boot profile. The options temporarily replace the options in the boot profile. Use this parameter only if advised to do so by D-Link.

**OPT+**=*option* String up to 128 bytes of boot options to pass to the booted system image in addition to the boot option(s) in the currently active boot profile. The options are appended to the options already in the boot profile. Use this parameter only if advised to do so by D-Link.

**Defaults:** The boot settings in the currently active boot profile are used by default.

**Access:** Boot prompt.

**Usage:** If you use an optional parameter, the parameter setting overrides the setting of the same parameter in the currently active boot profile. However, the boot profile itself is not changed. To display the currently active boot profile, use the **show** command. To change the currently active boot profile, use the **change** command.

**Examples:** The following command loads system image file MX010101.020 from boot partition 1:

```
boot> boot FN=MX010101.020 DEV=boot1
Compact Flash load from boot1:testcfg matches MX010101.020.
unzip: Inflating ramdisk_1.1.1.. OK
unzip file len 36085486 OK

Copyright (c) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003
The NetBSD Foundation, Inc. All rights reserved.

Copyright (c) 1982, 1986, 1989, 1991, 1993
The Regents of the University of California. All rights reserved.
Power Cycle Reboot
Detecting hardware...done.
readclock: 2003-10-8 2:9:50.67 UTC=>1065578990.670000 (1064992894)
init: Creating mfs /dev
erase ^H, werase ^W, kill ^U, intr ^C, status ^T
Doing D-Link mounts and links
Starting nos_mon...
nos_mon:ps: not found
SYSLOGD Oct 08 02:10:05.477814 CRITICAL SYSTEM_READY: The system has
finished booting.
Copyright (c) 2002, 2003
D-Link System, Inc.
Username:
Password:
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# change

Changes parameters in the currently active boot profile.

**Syntax:** change

**Defaults:** The default boot type is c (compact flash). The default filename is default. The default flags setting is 0x00000000 (all flags disabled) and the default options list is run=nos;boot=0. The default device setting is the boot partition specified by the most recent set boot partition command typed at the Enabled level of the CLI, or boot 0 if the command has never been typed.

**Access:** Boot prompt.

**Usage:** After you type the change command, the system interactively displays the current setting of each parameter and prompts you for the new setting. When prompted, type the new setting, press Enter to accept the current setting, or type . (period) to change the setting to its default value. To back up to the previous parameter, type - (hyphen).

**Examples:** The following command enters the configuration mode for the currently active boot profile, changes the device to boot1, and leaves the other parameters with their current settings:

```
boot> change
Changing the default configuration is not recommended.
Are you sure that you want to proceed? (y/n)y

BOOT TYPE:      [c]
DEVICE:         [boot0:]boot1
FILENAME:       [default]
FLAGS:          [0x00000000]
OPTIONS:        [run=nos;boot=0]
```

The following command enters the configuration mode for the currently active boot profile and configures the switch to boot using a TFTP server:

```
boot> change
Changing the default configuration is not recommended.
Are you sure that you want to proceed? (y/n)y

BOOT TYPE:      [c]> n
DEVICE:         [boot0:]> emac1
FILENAME:       [default]> bootfile
HOST IP:        [0.0.0.0]> 172.16.0.1
LOCAL IP:       [0.0.0.0]> 172.16.0.21
GATEWAY IP:     [0.0.0.0]> 172.16.0.20
IP MASK:        [0.0.0.0]> 255.255.255.0
FLAGS:          [0x00000000]>
OPTIONS:        [run=nos;boot=0]>
```


Download from Www.Somanuals.com. All Manuals Search And Download.

# create

Creates a new boot profile.

**Syntax: create**

**Defaults:** The new boot profile has the same settings as the currently active boot profile by default.

**Access:** Boot prompt.

**Usage:** A DWS-1008 switch can have up to four boot profiles. The boot profiles are stored in slots, numbered 0 through 3. When you create a new profile, the system uses the next available slot for the profile. If all four slots already contain profiles and you try to create a fifth profile, the switch displays a message advising you to change one of the existing profiles instead.

To make a new boot profile the currently active boot profile, use the next command. To change boot parameter settings, use the change command.

**Examples:** The following command creates a new boot profile in slot 1 on a switch that currently has only one boot profile, in slot 0:

```
boot> create
BOOT Index: 1
BOOT TYPE: c
DEVICE: boot1:
FILENAME: default
FLAGS: 00000000
OPTIONS: run=nos;boot=0
```

**See Also:**
- change
- delete
- next
- show


Download from Www.Somanuals.com. All Manuals Search And Download.

# delete

Removes the currently active boot profile.

**Syntax: delete**

**Defaults:** None.

**Access:** Boot prompt.

**Usage:** When you type the delete command, the next-lower numbered boot profile becomes the active profile. For example, if the currently active profile is number 3, profile number 2 becomes active after you type delete to delete profile 3. You cannot delete boot profile 0.

**Examples:** To remove the currently active boot profile, type the following command:

```
boot> delete
BOOT Index: 1
BOOT TYPE: c
DEVICE: boot1:
FILENAME: default
FLAGS: 00000000
OPTIONS: run=nos;boot=0
```

**See Also:**
- change
- create
- next
- show

# dhcp

Displays or changes the state of the DHCP option. The DHCP option controls whether a switch uses DCHP to obtain its IP address when it is booted using a TFTP server.

**Syntax: dhcp [ON | on | OFF | off]**

**ON** Enables the DHCP option.

**on** Same effect as ON.

**OFF** Disables the DHCP option.

**off** Same effect as OFF.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** The DHCP option is disabled by default.

**Access:** Boot prompt.

**Examples:** The following command displays the current setting of the DHCP option:

```
boot> dhcp
DHCP is currently enabled.
```

The following command disables the DHCP option:

```
boot> dhcp
DHCP is currently disabled.
```

**See Also:**
• boot

# diag

Accesses the diagnostic mode.

**Syntax: diag**

**Defaults**: The diagnostic mode is disabled by default.

**Access:** Boot prompt.

**Usage:** Access to the diagnostic mode requires a password, which is not user configurable. Use this mode only if advised to do so by D-Link.

# dir

Displays the boot code and system image files on a DWS-1008 switch.

**Syntax: dir [c: | d: | e: | f: | boot0 | boot1]**

**c:** Nonvolatile storage area containing boot partition 0 (primary).
**d:** Nonvolatile storage area containing boot partition 1 (secondary).
**e:** Primary partition of the flash card in the flash card slot.
**f:** Secondary partition of the flash card in the flash card slot.
**boot0** Boot partition 0.
**boot1** Boot partition 1.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Defaults:** None.

**Access:** Boot prompt.

**Usage:** To display the system image software versions, use the **fver** command. This command does not list the boot code versions. To display the boot code versions, use the version command.

**Examples:** The following command displays all the boot code and system image files on a DWS-1008 switch:

```
boot> dir

Internal Compact Flash Directory (Primary):
        MX010101.020            5523634 bytes
        BLOAD                   696176 bytes
        BSTRAP                  38056 bytes

        Internal Compact Flash Directory (Secondary):
        MX010101.020            5524593 bytes
```

**See Also:**
- fver
- version

# fver

Displays the version of a system image file installed in a specific location on a DWS-1008 switch.

**Syntax: fver {c: | d: | e: | f: | boot0: | boot1:} [***filename***]**

| | |
|---|---|
| **c:** | Nonvolatile storage area containing boot partition 0 (primary). |
| **d:** | Nonvolatile storage area containing boot partition 1 (secondary). |
| **e:** | Primary partition of the flash card in the flash card slot. |
| **f:** | Secondary partition of the flash card in the flash card slot. |
| **boot0:** | Boot partition 0. |
| **boot1:** | Boot partition 1. |
| [*filename*] | System image filename. |

**Defaults:** None.

**Access:** Boot prompt.

**Usage:** To display the image filenames, use the dir command. This command does not list the boot code versions. To display the boot code versions, use the version command.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** The following command displays the system image version installed in boot partition 1:

boot> **fver boot1**
File boot1:default version is 1.1.0.98.

**See Also:**
• dir
• version

# help

Displays a list of all the boot prompt commands or detailed information for an individual command.

**Syntax: help [**command-name**]**

*command-name* Boot prompt command.

**Defaults:** None.

**Access:** Boot prompt.

**Usage:** If you specify a command name, detailed information is displayed for that command. If you do not specify a command name, all the boot prompt commands are listed.

**Examples:** The following command displays detailed information for the **fver** command:

boot> **help fver**

fver Display the version of the specified device:filename.

USAGE: fver
[c:file|d:file|e:file|f:file|boot0:file|boot1:file|boot2:file|boot3:file]

Command to display the version of the compressed image file associated with the given device:filename.

**See Also:**
• ls


Download from Www.Somanuals.com. All Manuals Search And Download.

# ls

Displays a list of the boot prompt commands.

**Syntax: ls**

**Defaults:** None.

**Access:** Boot prompt.

**Usage:** To display help for an individual command, type help followed by the command name (for example, help boot).

**Examples:** To display a list of the commands available at the boot prompt, type the following command:

boot> **ls**

| | |
|---|---|
| ls | Display a list of all commands and descriptions. |
| help | Display help information for each command. |
| autoboot | Display the state of, enable, or disable the autoboot option. |
| boot | Load and execute an image using the current boot configuration profile. |
| change | Change the current boot configuration profile. |
| create | Create a new boot configuration profile. |
| delete | Delete the current boot configuration profile. |
| next | Select the next boot configuration profile. |
| show | Display the current boot configuration profile. |
| dir | Display the contents of the specified boot partition. |
| fver | Display the version of the loadable image specified by device:filename. |
| version | Display HW and Bootstrap/Bootloader version information. |
| reset | Reset the system. |
| test | Display the state of, enable, or disable the tests option. |
| diag | Access the diagnostic command CLI. |

**See Also:**
• help


Download from Www.Somanuals.com. All Manuals Search And Download.

# next

Activates and displays the boot profile in the next boot profile slot.

**Syntax:** next

**Defaults:** None.

**Access:** Boot prompt.

**Usage:** A DWS-1008 switch contains 4 boot profile slots, numbered 0 through 3. This command activates the boot profile in the next slot, in ascending numerical order.

If the currently active slot is 3, the command activates the boot profile in slot 0.

**Examples:** To activate the boot profile in the next slot and display the profile, type the following command:

```
boot> next
BOOT Index:     0
BOOT TYPE:      c
DEVICE:         boot1:
FILENAME:       testcfg
FLAGS:          00000000
OPTIONS:        run=nos;boot=0
```

**See Also:**
- change
- create
- delete
- show


Download from Www.Somanuals.com. All Manuals Search And Download.

# reset

Resets a DWS-1008 switch's hardware.

**Syntax:** reset

**Defaults:** None.

**Access:** Boot prompt.

**Usage:** After resetting the hardware, the reset command attempts to load a system image file only if other boot settings are configured to do so.

**Examples:** To immediately reset the system, type the following command at the boot prompt:

```
boot> reset

D-Link Systems Bootstrap 1.17 Release
Testing Low Memory 1 .....
Testing Low Memory 2 .....
CISTPL_VERS_1: 4.1 <SanDisk> <SDP> <5/3 0.6>
Reset Cause (0x02) is COLD

D-Link Systems Bootstrap/Bootloader
Version 1.6.5 Release
Bootstrap 0 version:        1.17   Active
Bootloader 0 version:       1.6.5  Active
Bootstrap 1 version:        1.17
Bootloader 1 version:       1.6.3

Board Revision:             3.
Controller Revision:        24.
POE Board Revision:         1
POE Controller Revision:    6

BOOT Index:                 0
BOOT TYPE:                  c
DEVICE:                     boot1:
FILENAME:                   default
FLAGS:                      00000000
OPTIONS:                    run=nos;boot=0
```

**See Also:**
• boot


Download from Www.Somanuals.com. All Manuals Search And Download.

# show

Displays the currently active boot profile. A boot profile is a set of parameters that a switch uses to control the boot process. Each boot profile contains the following parameters:

- **Boot type**—Either compact flash (local device on the switch) or network (TFTP)
- **Boot device**—Location of the system image file
- **Filename**—System image file
- **Flags**—Number representing the bit settings of boot flags to pass to the booted system image.
- **Options**—String up to 128 bytes of boot options to pass to the booted system image

A DWS-1008 switch can have up to four boot profiles, numbered 0 through 3. Only one boot profile can be active at a time. You can create, change, and delete boot profiles. You also can activate another boot profile in place of the currently active one.

**Syntax: show**

**Defaults:** None.

**Access:** Boot prompt.

**Examples:** To display the currently active boot profile, type the following command at the boot prompt:

```
boot> show
BOOT Index:       0
BOOT TYPE:        c
DEVICE: boot      1:
FILENAME:         default
FLAGS:            00000000
OPTIONS:          run=nos;boot=0
```

The following is an example of a boot profile that is booted with a software image downloaded from a TFTP server. In the example, when the switch boots, it downloads a system image file called bootfile located on a TFTP server with address 172.16.0.1.

```
boot> show
BOOT Index:       0
BOOT TYPE:        n
DEVICE:           emac1
FILENAME:         bootfile
HOST IP:          172.16.0.1
LOCAL IP:         172.16.0.21
GATEWAY IP:       172.16.0.20
IP MASK:          255.255.255.0
FLAGS:            00000000
OPTIONS:          run=nos
```


Download from Www.Somanuals.com. All Manuals Search And Download.

The table below describes the fields in the display.

| Field | Description |
|---|---|
| BOOT Index | Boot profile slot, which can be a number from 0 to 3. |
| BOOT TYPE | Boot type:<br>• c—Compact flash. Boots using nonvolatile storage or a flash card.<br>• n—Network. Boots using a TFTP server. |
| DEVICE | Location of the system image file:<br>• c:—Nonvolatile storage area containing boot partition 0<br>• d:—Nonvolatile storage area containing boot partition 1<br>• e:—Primary partition of the flash card in the flash card slot<br>• f:—Secondary partition of the flash card in the flash card slot<br>• boot0—boot partition 0<br>• boot1—boot partition 1<br><br>When the boot type is Network, the device can be one of the following:<br>• mgmt or tsec0—The 10/100 port labelled Mgmt |
| HOST IP | For network booting, the IP address of the host where the system image resides |
| LOCAL IP | For network booting, the IP address of the switch. If the DHCP option is enabled, this does not need to be specified. |
| GATEWAY IP | For network booting, the default router (gateway) used by the switch. If the DHCP option is enabled, this does not need to be specified. |
| IP MASK | For network booting, the subnet mask. If the DHCP option is enabled, this does not need to be specified. |
| FILENAME | System image file name. |
| FLAGS | Number representing the bit settings of boot flags to pass to the booted system image. |
| OPTIONS | String up to 128 bytes of boot options to pass to the booted system image. |

**See Also:**
- change
- create
- delete
- dhcp
- next


Download from Www.Somanuals.com. All Manuals Search And Download.

# test

Displays or changes the state of the poweron test flag. The poweron test flag controls whether an performs a set of self tests prior to the boot process.

**Syntax: test [ON | on | OFF | off]**

**ON** Enables the poweron test flag.

**on** Same effect as ON.

**OFF** Disables the poweron test flag.

**off** Same effect as OFF.

**Defaults:** The poweron test flag is disabled by default.

**Access:** Boot prompt.

**Examples:** The following command displays the current setting of the poweron test flag:

```
boot> test
The diagnostic execution flag is not set.
```

**See Also:**
• boot

# version

Displays version information for a switch's hardware and boot code.

**Syntax:** version

**Defaults:** None.

**Access:** Boot prompt.

**Usage:** This command does not list the system image file versions installed in the boot partitions. To display system image file versions, use the **dir** or **fver** command.


Download from Www.Somanuals.com. All Manuals Search And Download.

**Examples:** To display hardware and boot code version information, type the following command at the boot prompt:

```
boot> version

D-Link Systems Bootstrap/Bootloader
Version 1.6.5 Release

Bootstrap 0 version:        1.17 Active
Bootloader 0 version:       1.6.5 Active
Bootstrap 1 version:        1.17
Bootloader 1 version:       1.6.3
Board Revision:             3.
Controller Revision:        24.
POE Board Revision:         1
POE Controller Revision:    6
```

**See Also:**
- dir
- fver


Download from Www.Somanuals.com. All Manuals Search And Download.

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com