Dell PowerConnect Switch Command Reference

This manual describes the Command Line Interface.

March 2003

Back to Contents Page

Address Table Commands:
Dell PowerConnect Switch User's Guide

---

mac-address-table static

Use this command to map a static address to a port in a VLAN. Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address interface* **vlan** *vlan-id* [*action*]
no mac-address-table static *mac-address* **vlan** *vlan-id*

- *mac-address* - MAC address.
- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)
- *vlan-id* - VLAN ID (Range: 1-4094)
- *action* -
  - **delete-on-reset**: Assignment lasts until switch is reset.
  - **permanent**: Assignment is permanent.

Default Setting

No static addresses are defined. The default mode is **permanent**.

Command Mode

Global Configuration

Command Usage

- The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:
  - Static addresses will not be removed from the address table when a given interface link is down.
  - Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
  - A static address cannot be learned on another port until the address is removed with the **no** form of this command.
- The maximum number of address entries -
  - PowerConnect 3248: 8191
  - PowerConnect 5224: 32768

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de ethernet 1/1 vlan 1 delete-on-reset
Console(config)#
```

---

clear mac-address-table dynamic

Use this command to remove any learned entries from the forwarding database and to clear the transmit and receive counts for any static or system-configured entries.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear mac-address-table dynamic
```

```
Console#
```

show mac-address-table

Use this command to view classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

- mac-*address* - MAC address.
- *mask* - Bits to match in the address.
- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)
- *vlan-id* - VLAN ID (Range: 1-4094)
- **sort** - Sort by **address**, **vlan** or **interface**.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The MAC Address Table contains the MAC addresses associated with each interface.
- The Type field may include the following types:
  - Learned - dynamic address entries
  - Permanent - static entry
  - Delete-on-reset - static entry to be deleted when system is reset
- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit “0” means to match a bit and “1” means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means "any."
- The maximum number of address entries -
  - PowerConnect 3248: 8191
  - PowerConnect 5224: 32768

Example

```
Console#show bridge 1
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-10-b5-62-03-74    1 Learned
  Eth 1/ 7 00-e0-29-94-34-1d    1 Learned
Console#
```

mac-address-table aging-time

Use this command to set the aging time for entries in the address table. Use the **no** form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*
no mac-address-table aging-time

- *seconds* - Time is number of seconds
  (PowerConnect 5224: 17-2148; PowerConnect 3248: 10-1000000).

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 300
Console(config)#
```

---

show mac-address-table aging-time

Use this command to show the aging time for entries in the address table.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table aging-time
 Aging time: 300 sec.
Console#
```

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

Authentication Commands:
Dell PowerConnect Switch User's Guide

You can configure the switch to authenticate users logging into the system for management access using local or authentication-server methods.
Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS+-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

---

authentication login

Use this command to define the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

authentication login {[**local**] [**radius**] [**tacacs**]}
no authentication login

- **local** - Use local authentication.
- **radius** - Use RADIUS server authentication.
- **tacacs** - Use TACACS+ server authentication.

Default Setting

Local only

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server.
- RADIUS and TACACS+ logon authentication can control management access via the console port, a Web browser, or Telnet. These access options must be configured on the authentication server.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication login radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.
- If you are using only a RADIUS server for authentication, you need to configure a special user name on the server for the CLI **enable** command that allows access to the Privileged Exec level from the Normal Exec level. The user name to configure on the RADIUS server for this command is "$Enable."

Example

```
Console(config)#authentication login radius local
Console(config)#
```

Related Commands

username for setting the local password

---

radius-server host

Use this command to specify the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server host *host_ip_address*
no radius-server host

host_ip_address - IP address of a RADIUS server.

Default Setting

10.1.0.1

Command Mode

Global Configuration

Example

```
Console(config)#radius-server host 192.168.1.25
Console(config)#
```

---

radius-server port

Use this command to set the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server port *port_number*
no radius-server port

port_number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server port 181
Console(config)#
```

---

radius-server key

Use this command to set the RADIUS encryption key. Use the **no** form to restore the default.

Syntax

radius-server key *key_string*
no radius-server key

key_string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string.
(Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key solvent
Console(config)#
```

---

radius-server retransmit

Use this command to set the number of retries. Use the **no** form to restore the default.

Syntax

radius-server retransmit *number_of_retries*
no radius-server retransmit

number_of_retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range is 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5
Console(config)#
```

---

radius-server timeout

Use this command to set the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server timeout *number_of_seconds*
no radius-server timeout

number_of_seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5 seconds

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10
Console(config)#
```

---

show radius-server

Use this command to display current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show radius-server
Server IP address: 10.1.0.99
 Communication key with radius server: solvent
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5
Console#
```

---

tacacs-server host

Use this command to specify the RADIUS server. Use the **no** form to restore the default.

Syntax

tacacs-server host *host_ip_address*
no tacacs-server host

host_ip_address - IP address of a TACACS+ server.

Default Setting

10.11.12.13

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

---

tacacs-server port

Use this command to set the TACACS+ server network port. Use the **no** form to restore the default.

Syntax

radius-server port *port_number*
no radius-server port

port_number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181
Console(config)#
```

---

tacacs-server key

Use this command to set the TACACS+ encryption key. Use the **no** form to restore the default.

Syntax

tacacs-server key *key_string*
no tacacs-server key

key_string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string.
(Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server key green
Console(config)#
```

---

show tacacs-server

Use this command to display current settings for the TACACS+ server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show tacacs-server
Remote TACACS server configuration:
Server IP address: 10.11.12.13
Communication key with radius server: green
Server port number: 49
Console#
```

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

Broadcast Storm Control Commands: Dell PowerConnect Switch User's Guide

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then dropped. (Broadcast Storm Control is enabled by default.)

---

switchport broadcast

Use this command to configure broadcast storm control. Use the **no** form to disable broadcast storm control.

Syntax

switchport broadcast packet-rate *rate*
no switchport broadcast

rate - Threshold level as a rate; i.e., packets per second.
(Range - PowerConnect 5224: 16, 64, 128, 256; PowerConnect 3248: 500 - 262143)

Default Setting

- PowerConnect 5224: 256 packets per second
- PowerConnect 3248: 500 packets per second

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.
- This command can enable or disable broadcast storm control for the selected interface. However, the specified threshold value applies to the entire switch.
- Enabling jumbo frames for the PowerConnect 5224 will limit the maximum threshold for broadcast storm control to 64 packets per second. (See the jumbo frame command.)

Example

The following shows how to configure broadcast suppression at 64 packets per second on port 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 64
Console(config-if)#
```

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

Using the CLI:
Dell PowerConnect Switch Command Reference

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the switch's console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are "admin" and "guest" with corresponding passwords of "admin" and "guest.") When the administrator user name and password is entered, the CLI displays the "Console#" prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the "Console>" prompt and enters normal access mode (i.e., Normal Exec).
2. Enter the necessary commands to complete your desired tasks.
3. When finished, exit the session with the “quit” or "exit" command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification

Username: admin
Password:

CLI session with the PowerConnect is opened.
To end the CLI session, enter [Exit].

Console#
```

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address.

To access the switch through a Telnet session, you must first set the IP address for the switch, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.1 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps.

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the "Vty-0#" prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or "Vty-0>" for the guest to show that you are using normal access mode (i.e., Normal Exec).
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the "quit" or "exit" command.

After entering the Telnet command, the login screen displays:

```
User Access Verification

Username: admin
Password:
```

```
CLI session with the PowerConnect is opened.
To end the CLI session, enter [Exit].

Vty-0#
```

NOTE: You can open up to four sessions to the device via Telnet.

Setting Passwords

NOTE: If this is your first time to log into the configuration program, you should define a new password using the "username" command, record it and put it in a safe place.

Passwords can consist of up to 8 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name and password "admin" to access Privileged Exec mode.
2. Type "configure" and press <Enter>.
3. Type "username guest password 0 *password*," for the Normal Exec level, where *password* is your new password. Press <Enter>.
4. Type "username admin password 0 *password*," for the Privileged Exec level, where *password* is your new password. Press <Enter>.
5. Save your configuration changes by typing "copy running-config startup-config." Press <Enter>.

NOTE: CLI configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the startup configuration file using the copy command.

Setting an IP Address

You must assign an IP address to this device to gain management access over your network. You may also need to a establish a default gateway between this device and management stations that exist on another network segment. You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server when it is powered on. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

NOTE: The IP address for this switch is assigned via DHCP by default. The default management interface is VLAN 1.

If you select the "bootp" or "dhcp" option, IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).

```
Console#config
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
Console(config)#
```

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

- IP address for the switch
- Default gateway for the network
- Network mask for this network

To assign an IP address to the switch, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>.
2. Type "ip address ip-address netmask," where "ip-address" is the switch IP address and "netmask" the network mask for the network.
3. Type "exit" to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the default gateway for the network to which the switch belongs, type "ip default-gateway gateway," where "gateway" is the IP address of the default gateway. Press <Enter>.
5. Save your configuration changes by typing "copy running-config startup-config." Press <Enter>.

At this point, you are ready to use appropriate network cabling to connect devices to the switch's external RJ-45 connectors.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command "show interfaces status ethernet 1/5," **show**, **interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

NOTE: This switch is a standalone unit, so the interface or unit number is always "1." For example, you should enter "1/5" for port 5.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:
  Console>**enable**
  Console# **show startup-config**
- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:
  Console(config)# **username admin password 0 smith**

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command "configure" can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print remaining characters of a partial keyword up to the point of ambiguity. In the "configure" example, typing **con** followed by a tab will result in printing the command up to "**configure**."

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the "?" character to list keywords or parameters.

Showing Commands

If you enter a "?" at the command prompt, the system will display the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, Interface, Line, or VLAN Database). You can also display a list of valid keywords for a specific command. For example, the command "**show ?**" displays a list of possible show commands:

```
Console#show ?
  bridge-ext         Bridge extend information
  garp               Garp property
  gvrp               Show gvrp information of interface
  history            Information of history
  interfaces         Information of interfaces
  ip                 IP information
  line               TTY line information
  logging            Show the contents of logging buffers
  mac-address-table  Set configuration of the address table
  map                Map priority
  port               Characteristics of the port
  queue              Information of priority queue
  radius-server      Radius server information
  running-config     The system configuration of running
  snmp               SNMP statistics
  spanning-tree      Specify spanning-tree
  ssh                Secure shell
  startup-config     The system configuration of starting up
  system             Information of system
  tacacs-server      Login by tacacs server
  users              Display information about terminal lines
  version            System hardware and software status
  vlan               Switch VLAN Virtual Interface
Console#show
```

The command "show interfaces ?" will display the following information:

```
Console>show interfaces ?
  counters    Information of interfaces counters
  status      Information of interfaces status
  switchport  Information of switchport
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example "**s?**" shows all the keywords starting with "s."

```
Console#show s?
snmp            spanning-tree   ssh             startup-config   system
Console#show s
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword "**no**" to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark "?" at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Class	Mode
Exec	Normal Privileged
Configuration*	Global Interface Line VLAN

*You must be in Privileged Exec mode to access any of the configuration modes.

Exec Commands

When you open a new console session on switch with the user name "guest," the system enters Normal Exec command mode (or guest mode). Only a limited number of the commands are available in this mode. You can access all the commands only in Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name "admin," or enter the **enable** command (followed by the privileged level password if so configured). The command prompt displays as "Console>" for Normal Exec mode and "Console#" for Privileged Exec mode.

To enter Privileged Exec mode, enter the following commands and passwords:

```
Username: admin
Password: [system login password]

CLI session with the PowerConnect is opened.
To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [system login password]

CLI session with the PowerConnect is opened.
To end the CLI session, enter [Exit].

Console>enable
Password: [privileged level password if so configured]
Console#
```

Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in nonvolatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into three different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port configuration, and include command such as **parity** and **databits**.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to "Console(config)# " which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter Interface, Line Configuration, or VLAN mode, you must enter the "**interface** …," "**line** …" or "**vlan database**" command while in Global Configuration mode. The system prompt will change to "Console(config-if)#," "Console(config-line)#" or "Console(config-vlan)" indicating that you have access privileges to the associated commands. You can use the **end** command to return to the Privileged Exec mode.

```
Console(config)#interface ethernet 1/5
Console(config-if)#exit
Console(config)#line console
Console(config-line)#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the "?" character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Keystroke	**Function**
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-P	Shows the last command.
Ctrl-U	Deletes the entire line.
Ctrl-W	Deletes the last word typed.
Delete key or backspace key	Erases a mistake when entering a command.

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

Command Groups:
Dell PowerConnect Switch User's Guide

Command Groups

The system commands can be broken down into the functional groups shown below.

Command Group	Description
General	Basic commands for entering privileged access mode, restarting the system, or quiting the CLI
Flash/File	Manages code image or switch configuration files
System Management	Controls system logs, system passwords, user name, browser management options, and a variety of other system information
Authentication	Configures RADIUS and TACACS+ client-server authentication for logon access
GVRP	Configures GVRP settings that permit automatic VLAN learning
LACP	Configures Link Aggregation Control Protocol for port trunking
SNMP	Activates authentication failure traps; configures community access strings, and trap managers
Line	Sets communication parameters for the serial port, including baud rate and console time-out
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs
Address Table	Configures the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time
IP	Configures the IP address and gateway for management access, displays the default gateway, or pings a specified device
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port
Spanning Tree	Configures Spanning Tree settings for the switch
Bridge Extension	Enables GVRP multicast protocol; shows the configuration for bridge extension commands
Priority	Sets port priority for untagged frames, relative weight for each priority queue, and the maximum number of queues enabled; also sets priority for TCP/UDP traffic types, IP precedence, and DSCP
VLAN	Configures VLAN settings, and defines port membership for VLAN groups
Port Trunking	Aggregates multiple ports into a single logical trunk
IGMP Snooping	Configures IGMP multicast filtering, querier eligibility, query parameters, and specifies ports attached to a multicast router
Broadcast Storm Control	Configures broadcast storm control

Note that the access mode shown in the following tables is indicated by these abbreviations: NE (Normal Exec), PE (Privileged Exec), GC (Global Configuration), IE (Interface Configuration), LC (Line Configuration), and VC (VLAN Database Configuration).

General Commands

Command	Function	Mode
enable	Activates privileged mode	NE
disable	Returns to normal mode from privileged mode	PE
configure	Activates global configuration mode	PE
show history	Shows the command history buffer	NE, PE
reload	Restarts the system	PE
end	Returns to Privileged Exec mode	GC, IC, LC, VC
exit	Returns to the previous configuration mode, or exits the CLI	any
quit	Exits a CLI session	NE, PE
help	Shows how to use help	any
?	Shows options for command completion (context sensitive)	any

Flash/File Commands

Command	Function	Mode

copy	Copies a code image or a switch configuration to or from Flash memory or a TFTP server	PE
delete	Deletes a file or code image	PE
dir	Displays a list of files in Flash memory	PE
whichboot	Displays the files booted	PE
boot system	Specifies the file or image used to start up the system	GC

System Management Commands

Command	Function	Mode
hostname	Specifies or modifies the host name for the device	GC
username	Sets user name authentication at login	GC
enable password	Sets a password to control access to various privilege levels	GC
jumbo frame	Allows jumbo frames to pass through the switch	GC
ip http port	Specifies the port to be used by the Web browser interface	GC
ip http server	Allows the switch to be monitored or configured from a browser	GC
ip http secure-port	Specifies the UDP port number used for HTTPS connection to the switch's Web interface.	GC
ip http secure-server	Enables the HTTPS server on the switch.	GC
ip ssh server	Enables the SSH server on the switch.	GC
ip ssh	Specifies the authentication timeout for the SSH server and the number of retries allowed by a client.	GC
disconnect ssh	Terminates an SSH connection.	PE
logging on	Controls logging of error messages	GC
logging history	Limits syslog messages sent to the SNMP network management station based on severity	GC
logging host	Adds a syslog server host IP address that will receive logging messages.	GC
logging facility	Sets the facility type for remote logging of syslog messages.	GC
logging trap	Limits syslog messages saved to a remote server based on severity.	GC
clear logging	Clears messages from the logging buffer	PE
show startup-config	Displays the contents of the configuration file (stored in Flash memory) that is used to start up the system	PE
show running-config	Displays the configuration data currently in use	PE
show logging	Displays the state of logging	PE
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries.	PE
show ssh	Displays the status of current SSH sessions.	PE
show system	Displays system information	NE, PE
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client	NE, PE
show version	Displays version information for the system	NE, PE

Authentication Commands

Command	Function	Mode
authentication login	Defines logon authentication method and precedence	GC
radius-server host	Specifies the RADIUS server	GC
radius-server port	Sets the RADIUS server network port	GC
radius-server key	Sets the RADIUS encryption key	GC
radius-server retransmit	Sets the number of retries	GC
radius-server timeout	Sets the interval between sending authentication requests	GC
show radius-server	Displays current settings for the RADIUS server	PE
tacacs-server host	Specifies the TACACS+ server	GC
tacacs-server port	Specifies the TACACS+ server network port	GC
tacacs-server key	Sets the TACACS+ encryption key	GC
show tacacs-server	Shows the current TACACS+ settings	PE

GVRP Commands

Command	Function	Mode
show gvrp configuration	Displays GVRP configuration for selected interface	NE, PE
garp timer	Sets the GARP timer for the selected function	IC
show garp timer	Shows the GARP timer for the selected function	NE, PE

LACP Commands

Command	Function	Mode
lacp	Configures LACP for the current interface	IC

SNMP Commands

Command	Function	Mode
show snmp	Displays the status of SNMP communications	NE, PE
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC
snmp-server contact	Sets the system contact string	GC
snmp-server host	Specifies the recipient of an SNMP notification operation	GC
snmp-server location	Sets the system location string	GC
snmp-server enable traps	Enables the device to send SNMP traps or inform requests (i.e., SNMP notifications)	GC
snmp ip filter	Sets IP addresses of clients allowed to management access to the switch via SNMP.	GC

Line Commands

Command	Function	Mode
line	Identifies a specific line for configuration and starts the line configuration mode	GC
login	Enables password checking at login	LC
password	Specifies a password on a line	LC
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC
silent-time	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command	LC
databits	Sets the number of data bits per character that are interpreted and generated by hardware	LC
parity	Defines generation of a parity bit	LC
speed	Sets the terminal baud rate	LC
stopbits	Sets the number of the stop bits transmitted per byte	LC
show line	Displays a terminal line's parameters	NE, PE

Interface Commands

Command	Function	Mode
interface	Configures an interface type and enters interface configuration mode	GC
shutdown	Disables an interface	IC
clear counters	Clears statistics on an interface	PE
description	Adds a description to an interface configuration	IC
speed-duplex	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC
negotiation	Enables autonegotiation of a given interface	IC
capabilities	Advertises the capabilities of a given interface for use in autonegotiation	IC
flowcontrol	Enables flow control on a given interface	IC
port security	Enables port security on an interface.	IC
show interfaces status	Displays status for the specified interface	NE,

		PE
show interfaces counters	Displays statistics for the specified interface	NE, PE
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE

Address Table Commands

Command	Function	Mode
mac-address-table static	Maps a static address to a port in a VLAN	GC
clear mac-address-table dynamic	Removes any learned entries from the forwarding database and clears the transmit and receive counts for any statically or system configured entries	PE
show mac-address-table	Displays classes of entries in the bridge-forwarding database	PE
mac-address-table aging-time	Sets the aging time of the address table	GC
show mac-address-table aging-time	Shows the aging time for the address table	PE

IP Commands

Command	Function	Mode
ip address	Sets the IP address for this device	IC
ip dhcp restart	Submits a BOOTP or DCHP client request	PE
ip default-gateway	Defines the default gateway through which an in-band management station can reach this device	GC
show ip interface	Displays the IP settings for this device	PE
show ip redirects	Displays the default gateway configured for this device	PE
ping	Sends ICMP echo request packets to another node on the network	NE, PE

Mirror Port Commands

Command	Function	Mode
port monitor	Configures a mirror session	IC
show port monitor	Shows the configuration for a mirror port	PE

Spanning Tree Commands

Command	Function	Mode
spanning-tree	Enables the spanning tree protocol	GC
spanning-tree mode	Configures STP or RSTP mode	GC
spanning-tree forward-time	Configures the spanning tree bridge forward time	GC
spanning-tree hello-time	Configures the spanning tree bridge hello time	GC
spanning-tree max-age	Configures the spanning tree bridge maximum age	GC
spanning-tree priority	Configures the spanning tree bridge priority	GC
spanning-tree pathcost method	Configures the path cost method for RSTP	GC
spanning-tree transmission-limit	Configures the transmission limit for RSTP	GC
spanning-tree cost	Configures the spanning tree path cost of an interface	IC
spanning-tree port-priority	Configures the spanning tree priority of an interface	IC
spanning-tree portfast	Sets an interface to fast forwarding	IC
spanning-tree edge-port	Enables fast forwarding for edge ports	IC
spanning-tree protocol-migration	Re-checks the appropriate BPDU format	PE
spanning-tree link-type	Configures the link type for RSTP	IC
show spanning-tree	Shows spanning tree configuration for the overall bridge or a selected interface	PE

Bridge Extension Commands

Command	Function	Mode
bridge-ext gvrp	Enables GVRP	GC

show bridge-ext	Shows bridge extension configuration	PE

Priority Commands

Command	Function	Mode
switchport priority default	Sets a port priority for incoming untagged frames or the priority of frames sent by the device connected to the specified port	IC
queue bandwidth	Assign round-robin weights to the priority queues	GC
queue cos map	Assigns class of service values to the priority queues	IC
map ip port	Enables TCP/UDP class of service mapping	GC
map ip port	Maps TCP/UDP socket to a class of service	IC
map ip precedence	Enables IP precedence class of service mapping	GC
map ip precedence	Maps IP precedence value to a class of service	IC
map ip dscp	Enables IP DSCP class of service mapping	GC
map ip dscp	Maps IP DSCP value to a class of service	IC
show queue bandwidth	Assign round-robin weights to the priority queues	PE
show queue cos-map	Shows the class of service map	PE
show map ip port	Shows the IP port map	PE
show map ip precedence	Shows the IP precedence map	PE
show map ip dscp	Shows the IP DSCP map	PE
show interfaces switchport	Displays the administrative and operational status of an interface	PE

VLAN Commands

Command	Function	Mode
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC
vlan	Configures a VLAN, including VID, name and state	VC
interface vlan	Enters interface configuration mode for specified VLAN	IC
switchport ingress-filtering	Enables ingress filtering on an interface	IC
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC
switchport mode	Configures VLAN membership mode for an interface	IC
switchport gvrp	Enables GVRP for an interface	IC
switchport allowed vlan	Configures the VLANs associated with an interface	IC
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC
show vlan	Shows VLAN information	NE, PE
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE

Port Trunking Commands

Command	Function	Mode
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	GC
channel-group	Adds a port to a trunk	IC
show interfaces status port-channel	Shows trunk information	NE, PE

IGMP Snooping Commands

Command	Function	Mode
ip igmp snooping	Enables IGMP snooping	GC
ip igmp snooping vlan mrouter	Adds a multicast router port	GC
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC

ip igmp snooping query-count	Configures the query count	GC
ip igmp snooping query-interval	Configures the query interval	GC
ip igmp snooping query-max-response-time	Configures the report delay	GC
ip igmp snooping query-time-out	Configures the query timeout	GC
ip igmp snooping version	Configures the IGMP version for snooping	GC
show ip igmp snooping	Shows the IGMP snooping configuration	PE
show ip igmp snooping mrouter	Shows multicast router ports	PE
show bridge multicast	Shows the IGMP snooping MAC multicast list	PE

Broadcast Storm Control Commands

Command	Function	Mode
switchport broadcast	Configures broadcast storm control	IC
show interfaces switchport	Displays the administrative and operational status of a port.	NE, PE

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

Bridge Extension Commands:
Dell PowerConnect Switch User's Guide

This section describes how to enable GVRP, as well as how to display the default configuration settings for the Bridge Extension MIB.

---

bridge-ext gvrp

Use this command to enable GVRP. Use the **no** form to disable it.

Syntax

bridge-ext gvrp
no bridge-ext gvrp

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Example

```
Console(config)#bridge-ext gvrp
Console(config)#
```

---

show bridge-ext

Use this command to show the configuration for bridge extension commands.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show bridge-ext
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Enabled
 GMRP: Disabled
Console#
```

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

Flash/File Commands:
Dell PowerConnect Switch User's Guide

These commands are used to manage the system code or configuration files.

---

copy

Use this command to move (upload/download) a code image or configuration file between the switch's Flash memory and a TFTP server. When you save the system code or configuration settings to a file on a TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

Syntax

copy file {**file** | **running-config** | **startup-config** | **tftp**}
copy running-config {**file** | **startup-config** | **tftp**}
copy startup-config {**file** | **running-config** | **tftp**}
copy tftp {**file** | **running-config** | **startup-config | https-certificate**}

- **file** - Keyword that allows you to copy to/from a file.
- **running-config** - Keyword that allows you to copy to/from the current running configuration.
- **startup-config** - The configuration used for system initialization.
- **tftp** - Keyword that allows you to copy to/from a TFTP server.
- **https-certificate** - Copies an HTTPS certificate from an TFTP server to the switch.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The system prompts for data required to complete the copy command.
- The destination configuration file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the length of file name should be 1 to 31. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- You can load up to two code image files in the switch.The number of user-defined configuration files is limited only by available Flash memory space.
- You can use "Factory_Default_Config.cfg" as the source to copy from the factory default configuration file, but you cannot use "Factory_Default_Config.cfg" as the destination.
- To replace the startup configuration, you must use startup-config as the destination.
- The Boot ROM (i.e., diagnostic) image cannot be uploaded or downloaded from the TFTP server. You can only download this file via the console interface during system bootup. (Reset power to the switch, press Ctrl-F during bootup, and select the appropriate menu items to download the Boot ROM image.)

Example

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
1. config: 2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
/
Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name : startup
/
Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
/
Console#
```

---

delete

Use this command to delete a file or image.

Syntax

delete *filename*

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If the file type is boot-ROM or is used for system startup, then this file cannot be deleted.
- "Factory_Default_Config.cfg" cannot be deleted.

Example

This example shows how to delete the *test2.cfg* configuration file from Flash memory.

```
Console#delete test2.cfg
Console#
```

Related Commands

dir

---

dir

Use this command to display a list of files in Flash memory.

Syntax

dir [**boot-rom** | **config** | **opcode** [**:***filename*]]

The type of file or image to display includes:

- **boot-rom** - Boot ROM
- **config** - Configuration file
- **opcode** - Name of the file or image. If this file exists but contains errors, information on this file cannot be shown.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If you enter the command **dir** without any parameters, the system displays all files.
- File information is shown below:

Table 1. File Information

Column Heading	Description
file name	The name of the file.

file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
file size	The length of the file in bytes.

Example

The following example shows how to display all file information:

```
Console#dir
                      file name      file type startup size (byte)
------------------------------ -------------- ------- -----------
                      diag_0060 Boot-Rom image       Y      111360
                      run_01642 Operation Code       N     1074304
                       run_0200 Operation Code       Y     1083008
     Factory_Default_Config.cfg    Config File       N        2574
                        startup    Config File       Y        2710
-------------------------------------------------------------------
                                        Total free space:         0
Console#
```

whichboot

Use this command to display which files booted.

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows the information displayed by the **whichboot** command. See Table 1 for a description of the file information displayed by this command.

```
Console#whichboot
        file name      file type startup size (byte)
---------------- -------------- ------- -----------
        diag_0060 Boot-Rom image       Y      111360
         run_0200 Operation Code       Y     1083008
          startup    Config File       Y        2710
Console#
```

boot system

Use this command to specify the file or image used to start up the system.

Syntax

boot system {**boot-rom**| **config** | **opcode**}**:** *filename*

The type of file or image to set as a default includes:

- **boot-rom** - Boot ROM
- **config** - Configuration file
- **opcode** - Run-time operation code

The colon (:) is required.

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- A colon (:) is required after the specified file.

- If the file contains an error, it cannot be set as the default file.

Example

```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands

dir
whichboot

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

General Commands:
Dell PowerConnect Switch User's Guide

---

enable

Use this command to activate Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See Understanding Command Modes.

Syntax

enable [*level*]

level - Privilege level to log in to the device.
The device has two predefined privilege levels: **0**: Normal Exec, **15**: Privileged Exec.
Enter level 15 to access Privileged Exec mode.

Default Setting

Level 15

Command Mode

Normal Exec

Command Usage

- "super" is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the enable password command.)
- The "#" character is appended to the end of the prompt to indicate that the system is in Privileged Exec access mode.

Example

```
Console>enable
Console#
```

Related Commands

disable
enable password

---

disable

Use this command to return to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See Understanding Command Modes.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The ">" character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example

```
Console#disable
```

```
Console>
```

Related Commands

enable

---

configure

Use this command to activate Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, and VLAN Database Configuration. See Understanding Command Modes.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#configure
Console(config)#
```

Related Commands

end

---

show history

Use this command to show the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 20 commands.

Example

In this example, the **show history** command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

---

reload

Use this command to restart the system.

*NOTE: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the **copy running-config startup-config** command.*

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```

---

end

Use this command to return to Privileged Exec configuration mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

---

exit

Use this command to return to the previous configuration mode or exit the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

---

quit

Use this command to exit the configuration program.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The **quit** and **exit** commands can both exit the configuration program..

Example

This example shows how to quit a CLI session:

```
Console>quit

Press ENTER to start session

User Access Verification

Username:
```

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

GVRP Commands:
Dell PowerConnect Switch User's Guide

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. GVRP must be enabled on all the switches between participating hosts to allow the switches to create dynamic VLANs.

---

show gvrp configuration

Use this command to show if GVRP is enabled.

Syntax

show gvrp configuration [*interface*]

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows both global and interface-specific configuration.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show gvrp configuration
Whole system:
GVRP configuration: Enabled
Eth 1/ 1:
 Gvrp configuration: Enabled
Eth 1/ 2:
 Gvrp configuration: Enabled
Eth 1/ 2:
 Gvrp configuration: Disabled
.
.
.
```

---

garp timer

Use this command to set the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

Syntax

garp timer {**join** | **leave** | **leaveall**} *timer_value*
no garp timer {**join** | **leave** | **leaveall**}

- {**join** | **leave** | **leaveall**} - Which timer to set.
- *timer_value* - Value of timer.
  Range:
  - join: 20-1000 centiseconds
  - leave: 60-3000 centiseconds
  - leaveall: 500-18000 centiseconds

Default Setting

- join: 20 centiseconds
- leave: 60 centiseconds
- leaveall: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.
- Timer values must meet the following restrictions:
  - leave >= (2 x join)
  - leaveall > leave

CAUTION: Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP will not operate successfully.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

Related Commands

show garp timer

---

show garp timer

Use this command to show the GARP timers for the selected interface.

Syntax

show garp timer [*interface*]

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows all GARP timers.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
 Join timer: 20 sec.
 Leave timer: 60 sec.
 Leaveall timer: 1000 sec.

Console#
```

Related Commands

garp timer

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

Interface Commands:
Dell PowerConnect Switch User's Guide

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

---

interface

Use this command to configure an interface type and enter interface configuration mode. Use the **no** form to remove a trunk.

Syntax

interface *interface*
no interface port-channel *channel-id*

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)
  - **vlan** *vlan-id* (Range: 1-4094)

Default Setting

None

Command Mode

Global Configuration

Example

To specify the first Ethernet port, enter the following command:

```
Console(config)#interface ethernet 1/1
Console(config-if)#
```

---

shutdown

Use this command to disable an interface. To restart a disabled interface, use the **no** form.

Syntax

shutdown
no shutdown

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables Ethernet port 5.

```
Console(config)#interface ethernet 1/5
(config-if)#shutdown
(config-if)#
```

---

clear counters

Use this command to clear statistics on an interface.

Syntax

clear counters *interface*

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on Ethernet port 5.

```
Console#clear counters ethernet 1/5
Console#
```

---

description

Use this command to add a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*
no description

string - Comment or a description to help you remember what is attached to this interface.
(Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following example adds a description to Ethernet port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#description RD SW#3
Console(config-if)#
```

---

speed-duplex

Use this command to configure the speed and duplex mode of a given interface when auto-negotiation is disabled. Use the **no** form to restore the default.

Syntax

speed-duplex {**1000full | 100full | 100half | 10full | 10half**}
no speed-duplex

- **1000full** - Forces 1000 Mbps full-duplex operation
- **100full** - Forces 100 Mbps full-duplex operation
- **100half** - Forces 100 Mbps half-duplex operation
- **10full** - Forces 10 Mbps full-duplex operation
- **10half** - Forces 10 Mbps half-duplex operation

Default Setting

- Auto-negotiation is enabled by default.
- When auto-negotiation is disabled, the default speed-duplex setting is 100half for Fast Ethernet ports and 1000full for Gigabit Ethernet ports.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the **no negotiation** command to disable auto-negotiation on the selected interface.

Example

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation

negotiation

Use this command to enable auto-negotiation for a given interface. Use the **no** form to disable auto-negotiation.

Syntax

negotiation
no negotiation

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

If auto-negotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Example

The following example configures port 11 to use auto-negotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

capabilities

Use this command to advertise the port capabilities of a given interface during auto-negotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

capabilities {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}
no capabilities [**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**]

- **1000full** - Supports 1000 Mbps full-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation
- **10full** - Supports 10 Mbps full-duplex operation
- **10half** - Supports 10 Mbps half-duplex operation
- **flowcontrol** - Supports flow control
- **symmetric** - Transmits and receives pause frames for flow control (Gigabit ports only)

Default Setting

- Fast Ethernet - 10half, 10full, 100half, 100full
- Gigabit Ethernet - 10half, 10full, 100half, 100full, 1000full

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following example configures Ethernet port 5 capabilities to 100half, 100full and flow control.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

---

flowcontrol

Use this command to enable flow control. Use the **no** form to disable flow control.

Syntax

flowcontrol
no flowcontrol

Default Setting

Flow control enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port
- To force operation to the specified **flowcontrol** mode (i.e., on or off), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.
- Flow control can only work on those ports located in the same chip (i.e., cross-chip flow control will not work).
  - PowerConnect 5224 - SW1: 1-12; SW2: 13-24
  - PowerConnect 3248 - SW1: 1-24,49; SW2: 25-48,50

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

capabilities (flowcontrol, symmetric)

---

port security

Use this command to enable and configure port security on a port. Use the **no** form to disable port security or reset the intrusion action to the default.

Syntax

port security [**action** {**shutdown** | **trap** | **trap-and-shutdown**}]
no port security [**action**]

- **action** - Indicates the security action to be taken when a port security violation is detected.
  - **shutdown** - Disable the port only.
  - **trap** - Issue an SNMP trap message only.
  - **trap-and-shutdown** - Issue an SNMP trap message and disable the port.

Default Setting

Status: Disabled
Action: None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- If you enable port security, the switch will stop dynamically learning new addresses on the specified port. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.
- To use port security, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on a port for an initial training period, and then enable port security to stop address learning. Be sure you enable the learning function long enough to ensure that all valid VLAN members have been registered on the selected port.
- To add new VLAN members at a later time, you can manually add secure addresses with the **mac-address-table static** command, or turn off port security to reenable the learning function long enough for new VLAN members to be registered. Learning may then be disabled again, if desired, for security.
- A secure port has the following restrictions:
  - It cannot be connected to a network interconnection device.
  - It cannot be a member of a static trunk.
  - It can be configured as an LACP trunk port, but the switch does not allow the LACP trunk to be enabled.
- A port that is already configured as an LACP or static trunk port cannot be enabled as a secure port.
- If a port is disabled due to a security violation, it must be manually re-enabled by using the **no shutdown** command.
- PowerConnect 5224 restrictions:
  - The switch only supports the **trap-and-shutdown** security action.
  - Although the **port security action** command is an Interface Configuration command, it applies globally to all switch ports.

Example

This example sets the port security action and enables port security for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown
Console(config-if)#port security
Console(config-if)#
```

Related Commands

shutdown
mac-address-table static

---

show interfaces status

Use this command to display status for an interface.

Syntax

show interfaces status *interface*

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)
  - **vlan** *vlan-id* (Range: 1-4094)

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

```
Console#show interfaces status ethernet 1/11
Information of Eth 1/11
 Basic information:
  Port type: 100tx
  Mac address: 00-00-e8-00-00-0a
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Broadcast storm: Enabled
  Broadcast storm limit: 500 packets/second
  Flow control: Disabled
  Lacp: Disabled
  Port security: Disabled
  Port security action: None
 Current status:
  Link status: Down
  Operation speed-duplex: 100full
  Flow control type: None
Console#
```

---

show interfaces counters

Use this command to display statistics for an interface.

Syntax

show interfaces counters *interface*

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

```
Console#show interfaces counters ethernet 1/11
Ethernet 1/11
 Iftable stats:
  Octets input: 19648, Octets output: 714944
  Unitcast input: 0, Unitcast output: 0
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 10524
  Broadcast input: 136, Broadcast output: 0
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
```

```
  Frame too longs: 0, Carrier sense errors: 0
 RMON stats:
  Drop events: 0, Octets: 734720, Packets: 10661
  Broadcast pkts: 136, Multi-cast pkts: 10525
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 9877, Packet size 65 to 127 octets: 93
  Packet size 128 to 255 octets: 691, Packet size 256 to 511 octets: 0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

---

show interfaces switchport

Use this command to display advanced interface configuration settings.

Syntax

show interfaces switchport [*interface*]

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. The items displayed by this command include:

- Broadcast threshold – Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level.
- Lacp status – Shows if Link Aggregation Control Protocol has been enabled or disabled.
- VLAN membership mode – Indicates membership mode as Trunk or Hybrid.
- Ingress rule – Shows if ingress filtering is enabled or disabled.
- Acceptable frame type – Shows if acceptable VLAN frames include all types or tagged frames only.
- Native VLAN – Indicates the default Port VLAN ID.
- Priority for untagged traffic – Indicates the default priority for untagged frames.
- Gvrp status – Shows if GARP VLAN Registration Protocol is enabled or disabled.
- Allowed Vlan – Shows the VLANs this interface has joined, where “(u)” indicates untagged and “(t)” indicates tagged.
- Forbidden Vlan – Shows the VLANs this interface can not dynamically join via GVRP.

Example

This example shows the configuration setting for Ethernet port 11.

```
Console#show interfaces switchport ethernet 1/11
Information of Eth 1/11
 Broadcast threshold: Enabled, 500 packets/second
 Lacp status: Enabled
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Enabled
 Allowed Vlan: 1(u),
 Forbidden Vlan:
Console#
```

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

IP Commands:
Dell PowerConnect Switch User's Guide

The factory default configuration is set to use DHCP for VLAN 1, with address 0.0.0.0 and subnet mask 255.0.0.0. The address obtained from the DHCP server may be used for management access over your network. If necessary, you can manually configure a new address. You may also need to a establish a default gateway between this device and management stations that exist on another network segment.

---

ip address

Use this command to set the IP address for this device. Use the **no** form to restore the default IP address.

Syntax

ip address {*ip-address netmask* | **bootp** | **dhcp**}
no ip address

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **bootp** - Obtains IP address from BOOTP.
- **dhcp** - Obtains IP address from DHCP.

Default Setting

None

Command Mode

Interface Configuration (VLAN)

Command Usage

- You must assign an IP address to this device to gain management access over the network. You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.
- If you select the **bootp** or **dhcp** option, IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).
- You can start broadcasting BOOTP or DHCP requests by entering an **ip dhcp restart** command, or by rebooting the switch.

NOTE: Only one VLAN interface can be assigned an IP address (the default is VLAN 1). This defines the management VLAN, the only VLAN through which you can gain management access to the switch. If you assign an IP address to any other VLAN, the new IP address overrides the original IP address and this becomes the new management VLAN.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

Related Commands

ip dhcp restart

---

ip dhcp restart

Use this command to submit a BOOTP or DCHP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- DHCP requires the server to reassign the client's last address if available.
- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
IP interface vlan
 IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
 and address mode: Dhcp.
Console#
```

Related Commands

ip address

---

ip default-gateway

Use this command to a establish a static route between this device and management stations that exist on another network segment. Use the **no** form to remove the static route.

Syntax

ip default-gateway *gateway*
no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No static route is established.

Command Mode

Global Configuration

Command Usage

A gateway must be defined if the management station is located in a different IP segment.

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

Related Commands

show ip redirects

---

show ip interface

Use this command to display the settings of an IP interface.

Default Setting

All interfaces

Command Mode

Privileged Exec

Command Usage

This switch can only be assigned one IP address. This address is used for managing the switch.

Example

```
Console#show ip interface
 IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#
```

Related Commands

show ip redirects

---

show ip redirects

Use this command to show the default gateway configured for this device.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

Related Commands

ip default-gateway

---

ping

Use this command to send ICMP echo request packets to another node on the network.

Syntax

ping *host* [**count** *count*][**size** *size*]

- *host* - IP address or IP alias of the host.
- *count* - Number of packets to send. (Range: 1-16, default: 5)
- *size* - Number of bytes in a packet. (Range: 32-512)
  The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

Default Setting

This command has no default for the host.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- Following are some results of the **ping** command:
  - *Normal response* -The normal response occurs in one to ten seconds, depending on network traffic.
  - *Destination does not respond* - If the host does not respond, the switch displays "timeout."
  - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
  - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- Press **<Esc>** to stop pinging.

Example

```
Console#ping 10.1.0.19
Type ESC to abort.
PING to 10.1.0.19, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 0 ms
response time: 10 ms
```

```
response time: 10 ms
response time: 10 ms
response time: 10 ms
Ping statistics for 10.1.0.19:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

Related Commands

interface

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

LACP Commands:
Dell PowerConnect Switch User's Guide

Link Aggregation Control Protocol (LACP) can be used to automatically negotiate a trunk link between this switch and another network device.

---

lacp

Use this command to enable 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

Syntax

lacp
no lacp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Finish configuring port trunks before you connect the corresponding network cables between switches.
- You can configure up to six trunks. The maximum number of ports that can be combined as a dynamic LACP trunk - PowerConnect 3248: 4 10/100 Mbps ports, 2 1000 Mbps ports; PowerConnect 5224: 6 1000 Mbps ports.
- All ports in the same trunk must consist of the same media type (i.e., twisted-pair or fiber).
- The ports on both ends of trunk must be configured the same for speed and flow control.
- The ports on both ends of trunk must also be configured for full duplex, either by forced mode or auto-negotiation.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated.
- If more than four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- STP, VLAN and IGMP settings can only be made for the entire trunk via the specified port-channel.
- Any trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.

Example

The following shows LACP enabled on ports 11 - 13. Because LACP has also been enabled on the ports at the other end of the links, the **show interfaces status port-channel 1** command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type: 100tx
  Mac address: 00-00-e8-00-00-0b
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Flow control status: Disabled
  Port security: Disabled
  Port security action: None
 Current status:
  Created by: lacp
  Link status: Up
  Operation speed-duplex: 100full
  Flow control type: None
  Member Ports: Eth1/11, Eth1/12, Eth1/13,
Console#
```

Back to Contents Page

Back to Contents Page

Line Commands:
Dell PowerConnect Switch User's Guide

You can access the onboard configuration program by attaching a VT100 compatible device to the switch's serial port. These commands are used to set communication parameters for the serial port or a virtual terminal. Note that Telnet is considered a virtual terminal connection, and the only commands that apply to Telnet include exec-timeout and password-thresh.

---

line

Use this command to identify a specific line for configuration, and to process subsequent line configuration commands.

Syntax

line {**console** | **vty**}

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access.

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

- This switch supports one console session, and up to four Telnet sessions.
- Telnet is considered a virtual terminal connection and will be shown as "Vty" in screen displays such as **show users**. However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

Related Commands

show line
show users

---

login

Use this command to enable password checking at login. Use the **no** form to disable password checking and allow connections without a password.

Syntax

login [**local**]
no login

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Default Setting

By default, virtual terminals require a password. If you do not set a password for a virtual terminal, it will respond to attempted connections by displaying an error message and closing the connection.

Command Mode

Line Configuration

Command Usage

If you specify **login** without the **local** option, authentication is based on the password specified with the **password** line configuration command.

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

username
password

---

password

Use this command to specify the password for a line. Use the **no** form to remove the password.

Syntax

password {**0** | **7**} *password*
no password

- {**0** | **7**} - 0 means plain password, 7 means encrypted password
- *password* - Character string that specifies the line password. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the **password-thresh** command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

login
password-thresh

---

exec-timeout

Use this command to set the interval that the system waits until user input is detected. Use the **no** form to remove the timeout definition.

Syntax

exec-timeout *seconds*
no exec-timeout

seconds - Integer that specifies the number of seconds. (Range: 0 - 65535 seconds; 0: no timeout)

Default Setting

Console - No timeout
Telnet - 600 seconds (10 minutes)

Command Mode

Line Configuration

Command Usage

- If no input is detected, the system resumes the current connection; or if no connections exist, it returns the terminal to the idle state and disconnects the incoming session.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

---

password-thresh

Use the **password-thresh** to set the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

password-thresh *threshold*
no password-thresh

threshold - The number of allowed password attempts. (Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

- When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. Use the **silent-time** command to set this interval.
- This command applies to both the local console and Telnet connections.

Example

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

Related Commands

silent-time

---

silent-time

Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command. Use the **no** form to remove the silent time value.

Syntax

silent-time *time*
no silent-time

time - The number of seconds to disable console response. (Range: 0-65535; 0: no silent-time)

Default Setting

The default value is no silent-time.

Command Mode

Line Configuration

Command Usage

If the password threshold was not set with the **password-thresh** command, silent-time begins after the default value of three failed logon attempts.

Example

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Related Commands

password-thresh

---

databits

Use this command to set the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

Syntax

databits {**7** | **8**}
no databits

- **7** - Seven data bits per character.
- **8** - Eight data bits per character.

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

Example

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

Related Commands

parity

---

parity

Use this command to define generation of a parity bit. Use the **no** form to restore the default setting.

Syntax

parity {**none** | **even** | **odd**}
no parity

- **none** - No parity
- **even** - Even parity
- **odd** - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Command Usage

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify no parity, enter this command:

```
Console(config-line)#parity none
Console(config-line)#
```

---

speed

Use this command to set the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

Syntax

speed *bps*
no speed

bps - Baud rate in bits per second. (Options: 9600, 57600, 38400, 19200, 115200 bps)

Default Setting

9600 bps

Command Mode

Line Configuration

Command Usage

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported.

Example

To specify 57600 bps, enter this command:

```
Console(config-line)#speed 57600
Console(config-line)#
```

---

stopbits

Use this command to set the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

Syntax

stopbits {**1** | **2**}

- **1** - One stop bit
- **2** - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

---

show line

Use this command to display the terminal line's parameters.

Syntax

show line [**console** | **vty**]

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access.

Default Setting

Show all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```
Console#show line
 Console configuration:
  Password threshold: 3 times
  Interactive timeout: Disabled
  Silent time: Disabled
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1

 Vty configuration:
  Password threshold: 3 times
  Interactive timeout: 65535 sec
Console#
```

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

Mirror Port Commands:
Dell PowerConnect Switch User's Guide

This section describes how to mirror traffic from a source port to a target port.

---

port monitor

Use this command to configure a mirror session. Use the **no** form to clear a mirror session.

Syntax

port monitor *interface* [**rx** | **tx** | **both**]
no port monitor *interface*

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
- **rx** - Mirror received packets.
- **tx** - Mirror transmitted packets.
- **both** - Mirror both received and transmitted packets.

Default Setting

No mirror session is defined. When enabled, the default mirroring is for both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Command Usage

- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- The destination port is set by specifying an Ethernet interface.
- When mirroring port traffic, the destination port must be included in the same VLAN as the source port. See VLAN Commands.
- There are some differences in the mirror implementation for the PowerConnect switches:
  - PowerConnect 3248: You can create up to nine sessions, each with one or more source ports and one destination port. However, you should avoid sending too much traffic to the destination port from multiple source ports. Also, the source and destination port have to be either both in the port range 1-24 or 49 or both in the port range 25-48 or 50.
  - PowerConnect 5224: You can create a single session, with one source port and one destination port. Also, the source and destination port have to be either both in the port range 1-12 or both in the port range 13-24.

Example

The following example configures the switch to mirror all packets from port 5 to port 6:

```
Console(config)#interface ethernet 1/6
Console(config-if)#port monitor ethernet 1/5 both
Console(config-if)#
```

Related Commands

show port monitor

---

show port monitor

Use this command to display mirror information.

Syntax

show port monitor [*interface*]

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.

Default Setting

Shows all defined sessions.
(For maximum number of sessions, see port monitor.)

Command Mode

Privileged Exec

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port):Eth1/ 1
 Source port(monitored port)  :Eth1/ 6
 Mode                         :RX/TX

Console#
```

Related Commands

port monitor

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

Priority Commands:
Dell PowerConnect Switch User's Guide

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues.

---

switchport priority default

Use this command to set a priority for incoming untagged frames, or the priority of frames received by the device connected to the specified interface. Use the **no** form to restore the default value.

Syntax

switchport priority default *default-priority-id*
no switchport priority default

default-priority-id - The priority number for untagged ingress traffic.
The priority is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero. .

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- This switch provides four priority queues for each port. It is configured to use Weighted Round Robin, which can be viewed with the **queue bandwidth** command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 0 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
```

---

queue bandwidth

Use this command to assign weighted round-robin (WRR) weights to the four class of service (CoS) priority queues. Use the **no** form to restore the default weights.

Syntax

queue bandwidth *weight1…weight4*
no queue bandwidth

weight1...weight4 - The ratio of weights for queues 0 - 3 determines the weights used by the WRR scheduler. (Range: 1 - 255)

Default Setting

PowerConnect 3248: Weights 1, 4, 16 and 64 are assigned to queue 0, 1, 2 and 3 respectively
PowerConnect 5224: Weights 16, 64, 128 and 240 are assigned to queue 0, 1, 2 and 3 respectively

Command Mode

Global Configuration

Command Usage

WRR allows bandwidth sharing at the egress port by defining scheduling weights.

Example

The following example shows how to assign WRR weights of 1, 3, 5 and 7 to the CoS priority queues 0, 1, 2 and 3:

```
Console(config)#queue bandwidth 1 3 5 7
Console(config)#
```

Related Commands

show queue bandwith

---

queue cos-map

Use this command to assign class of service (CoS) values to the CoS priority queues. Use the **no** form set the CoS map to the default values.

Syntax

queue cos-map *queue_id* [*cos1 ... cosn*]
no queue cos-map

- *queue_id* - The queue ID of the CoS priority queue.
  Ranges are 0 to 3, where 3 is the highest CoS priority queue.
- *cos1 .. cosn* - The CoS values that are mapped to the queue id. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

Default Setting

This switch supports Class of Service by using four priority queues, with Weighted Round Robin for each port. Up to 8 separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

Table 1. Priority to Queue Mapping

	Queue			
	0	**1**	**2**	**3**
Priority		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

CoS assigned at the ingress port is used to select a CoS priority at the egress port.

Example

The following example shows how to map CoS values 0, 1 and 2 to CoS priority queue 0, value 3 to CoS priority queue 1, values 4 and 5 to CoS priority queue 2, and values 6 and 7 to CoS priority queue 3:

```
Console(config)#interface ethernet 1/7
```

```
Console(config-if)#queue cos-map 0 0 1 2
Console(config-if)#queue cos-map 1 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#
```

Related Commands

show queue cos-map

---

map ip port (Global Configuration)

Use this command to enable IP port mapping (i.e., class of service mapping for TCP sockets). Use the **no** form to disable IP port mapping.

Syntax

map ip port
no map ip port

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- This command is not supported for the PowerConnect 5224.

Example

The following example shows how to enable TCP port mapping globally:

```
Console(config)#map ip port
Console(config)#
```

---

map ip port (Interface Configuration)

Use this command to set IP port priority (i.e., TCP port priority). Use the **no** form to remove a specific setting.

Syntax

map ip port *port-number* **cos** *cos-value*
no map ip port *port-number*

- *port-number* - 16-bit TCP port number. (Range: 1-65535)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- This command is not supported for the PowerConnect 5224.

Example

The following example shows how to map HTTP traffic to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#
```

---

map ip precedence (Global Configuration)

Use this command to enable IP precedence mapping (i.e., IP Type of Service). Use the **no** form to disable IP precedence mapping.

Syntax

map ip precedence
no map ip precedence

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP precedence mapping globally:

```
Console(config)#map ip precedence
Console(config)#
```

---

map ip precedence (Interface Configuration)

Use this command to set IP precedence priority (i.e., IP Type of Service priority). Use the **no** form to restore the default table.

Syntax

map ip precedence *ip-precedence-value* **cos** *cos-value*
no map ip precedence

- *precedence-value* - 3-bit precedence value. (Range: 0-7)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The table below shows the default priority mapping.

Table 2. IP Precedence to CoS Mapping

IP Precedence Value	CoS Value
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence values are mapped to default Class of Service values on a one-to-one basis according to recommendations in the IEEE 802.1p standard, and then mapped to the queue defaults shown in Table 1.
- This command sets the IP Precedence for all interfaces.

Example

The following example shows how to map IP precedence value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

map ip dscp (Global Configuration)

Use this command to enable IP DSCP mapping (i.e., Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

Syntax

map ip dscp
no map ip dscp

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```

map ip dscp (Interface Configuration)

Use this command to set IP DSCP priority (i.e., Differentiated Services Code Point priority). Use the **no** form to restore the default table.

Syntax

map ip dscp *dscp-value* **cos** *cos-value*
no map ip dscp

- *dscp-value* - 8-bit DSCP value. (Range: 0-255)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The table below shows the default priority mapping.

Table 3. DSCP to CoS Mapping

DSCP	CoS	DSCP	CoS	DSCP	CoS	DSCP	CoS	DSCP	CoS	DSCP	CoS	DSCP	CoS	DSCP	CoS
0	0	8	1	16	2	24	3	32	4	40	5	48	6	56	7
1	0	9	0	17	0	25	0	33	0	41	0	49	0	57	0
2	0	10	2	18	3	26	4	34	4	42	5	50	0	58	0
3	0	11	0	19	0	27	0	35	0	43	0	51	0	59	0
4	0	12	2	20	3	28	4	36	4	44	6	52	0	60	0
5	0	13	0	21	0	29	0	37	0	45	0	53	0	61	0
6	0	14	2	22	3	30	4	38	5	46	7	54	0	62	0
7	0	15	0	23	0	31	0	39	0	47	0	55	0	63	0

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard as shown in the following table, and then mapped to the queue defaults shown in Table 3.
- This command sets the DSCP Priority for all interfaces.

Example

The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

---

show queue bandwidth

Use this command to display the weighted round-robin (WRR) bandwidth allocation for the four class of service (CoS) priority queues.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue bandwidth
 Queue ID Weight
 -------- ------
        0      1
        1      4
        2     16
        3     64
Console#
```

---

show queue cos-map

Use this command to show the class of service priority map.

Syntax

show queue cos-map [*interface*]

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue cos-map ethernet 1/11
Information of Eth 1/11
 Queue ID Traffic class
 -------- -------------
    0     1 2
    1     0 3
    2     4 5
    3     6 7
Console#
```

---

show map ip port

Use this command to show the IP port priority map.

Syntax

show map ip port [*interface*]

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

The following shows that HTTP traffic has been mapped to CoS value 0:

```
Console#show map ip port
TCP port mapping status: disabled

 Port      Port no. COS
 --------- -------- ---
 Eth 1/ 5        80   0
Console#
```

Related Commands

map ip port - Maps CoS values to IP ports (i.e., TCP/UDP ports).

---

show map ip precedence

Use this command to show the IP precedence priority map.

Syntax

show map ip precedence [*interface*]

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip precedence
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
 Eth 1/ 5           0   0
 Eth 1/ 5           1   1
 Eth 1/ 5           2   2
 Eth 1/ 5           3   3
 Eth 1/ 5           4   4
 Eth 1/ 5           5   5
 Eth 1/ 5           6   6
 Eth 1/ 5           7   7
Console#
```

Related Commands

map ip precedence - Maps CoS values to IP precedence values.

show map ip dscp

Use this command to show the IP DSCP priority map.

Syntax

show map ip dscp [*interface*]

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

 Port       DSCP COS
 --------- ---- ---
 Eth 1/ 1     0   0
 Eth 1/ 1     1   0
 Eth 1/ 1     2   0
 Eth 1/ 1     3   0
 .
 .
 .
 Eth 1/ 1    61   0
 Eth 1/ 1    62   0
 Eth 1/ 1    63   0
Console#
```

Related Commands

map ip dscp - Maps CoS values to IP DSCP values.

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

Port Security Commands:
Dell PowerConnect Switch User's Guide

---

port security

Use this command to configure a secure port. Use the **no** form to disable port security.

Syntax

port security [**max-mac-count** *addresses*] | [**state** {**static** | **learning**}]
no port security

- *addresses* - The maximum number of secure addresses allowed on this port. (1-255)
- **static** - Only allows static addresses to be assigned to this port (using **bridge address secure**).
- **learning** - Learns the specified number of addresses as permanent entries.

Default Setting

All port security is disabled.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Setting the **state** clears the MAC address table for the port specified with the **interface** command.
- A secure port has the following restrictions:
  - Cannot use port monitoring.
  - Cannot be a multi-VLAN interface.
  - Cannot be connected to a network interconnection device.
  - Cannot be a trunk port.

Example

The following sets port 5 to use up to 100 addresses, and then sets the state to learning:

```
Console(config)# interface ethernet 1/5
Console(config-if)# port security max-mac-count 100
Console(config-if)# port security state learning
Console(config-if)#
```

Related Commands

bridge address secure

---

bridge address secure

Use this command to add a secure address to a port. Use the **no** form to clear an address.

Syntax

bridge *bridge-group* **address** *address* **secure** *interface* [**vlan** *vlan*]
no bridge *bridge-group* **address** *address* **secure** *interface* [**vlan** *vlan*]

- *bridge-group* - Bridge group index (bridge 1)
- address - MAC address
- *interface* - *type unit/port*
  - *type* - Type of interface (**ethernet**).
  - *unit* - This is device 1.
  - *port* - Port number.
- *vlan_id* - VLAN ID (Range: 1-2048)

Default Setting

No secure addresses

Command Mode

Global Configuration

Command Usage

- A secure address cannot be learned on another port until port security is disabled or the address is removed with the **clear bridge** command.
- If an entry already exists for the specified address and VLAN in another port's address table, it is first removed from that port and then assigned it to the specified port.

Example

The following adds the secure address 00-00-E8-11-22-33 to port 5:

```
Console(config)# bridge 1 address 00-00-E8-11-22-33 secure ethernet 1/5
Console(config)#
```

Related Commands

clear bridge

---

show bridge secure

Use this command to show port security information.

Syntax

show bridge *bridge-group* [*interface*] [*address* [*mask*]] **secure** [**sort** {**address** | **vlan** | **interface**}]

- *bridge-group* - Bridge group index
- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
- *address* - MAC address
- *mask* - Bits to ignore in the address.
- **sort** - Sort by **address**, **vlan** or **interface**. ???

Default Setting

Shows all secure addresses for the specified bridge group, sorted by address.

Command Mode

Privileged Exec

Example

The following shows the secure addresses for port 1:

```
Console#show bridge 1 secure sort address
Unit Port Vlan    Mac Address       Port Type
---- ---- ---- ------------------ -------------
 1    1    1    00-00-00-00-01-00        Dynamic
 1    1    1    00-00-00-01-00-E0        Dynamic
 1    1    1    00-00-01-00-E0-29        Dynamic
 1    1    1    00-01-00-E0-29-94        Dynamic
 1    1    1    00-20-29-94-34-1D        Dynamic
 1    1    1    00-E0-29-94-34-9D        Dynamic
 1    1    1    00-E0-29-94-34-DD        Dynamic
 1    1    1    00-E0-29-94-B4-1D        Dynamic
 1    1    1    00-E0-29-94-B4-DD        Dynamic
 1    1    1    00-E0-29-94-B4-FD        Dynamic
 1    1    1    A4-24-02-00-00-10        Dynamic
Console#
```

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

SNMP Commands:
Dell PowerConnect Switch User's Guide

These commands control access to this switch from SNMP management stations, as well as the error types sent to trap managers.

---

show snmp

Use this command to check the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides counter information for SNMP operations.

Example

```
Console#show snmp

SNMP traps:
 Authentication: enable
  Link-up-down: enable

SNMP communities:
   1. private, and the privilege is read-write
   2. public, and the privilege is read-only

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP logging: disabled
SNMP ip filter group:
    1. IP:10.1.2.3 Mask:255.255.255.255 valid
    2. IP:10.1.3.0 Mask:255.255.255.0 valid
Console#
```

---

snmp-server community

Use this command to define the community access string for the Simple Network Management Protocol. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro**|**rw**]

no snmp-server community *string*

- *string* - Community string that acts like a password and permits access to the SNMP protocol.
  (Maximum number of strings: 5; Maximum string length: 32 characters, case sensitive)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- public - read-only access. Authorized management stations are only able to retrieve MIB objects.
- private - with read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Command Usage

The first **snmp-server community** command you enter enables SNMP (SNMP v1 and SNMP v2c). The **no snmp-server community** command disables all versions of SNMP.

Example

```
Console(config)#snmp-server community private rw
Console(config)#
```

---

snmp-server contact

Use this command to set the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact *string*
no snmp-server contact

string - String that describes the system contact information.
(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands

snmp-server location

---

snmp-server location

Use this command to set the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*
no snmp-server location

text - String that describes the system location.
(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server location WC-19
Console(config)#
```

Related Commands

snmp-server contact

---

snmp-server host

Use this command to specify the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

Syntax

snmp-server host {*host-addr community-string*} [**version 1** | **2c**]
no snmp-server host *host-addr*

- *host-addr* - Name or Internet address of the host (the targeted recipient).
  (Maximum host addresses: 5 trap destination IP address entries)
- *community-string* - Password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.
  (Maximum length: 32 characters)
- **version** - Specifies whether to send notifications as SNMP v1 or SNMP v2c traps.

Default Setting

Host Address: None
SNMP Version: 1

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host
- The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.
- The switch can send SNMP version 1 or version 2c traps to a host IP address, depending on the SNMP version that the management station supports. If the **snmp-server host** command does not specify the SNMP version, the default is to send SNMP version 1 traps.
- Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.

Example

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

Related Commands

snmp-server enable traps

---

snmp-server enable traps

Use this command to enable this device to send Simple Network Management Protocol traps (SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

snmp-server enable traps [**authentication** | **link-up-down**]
no snmp-server enable traps [**authentication** | **link-up-down**]

- **authentication** - Keyword to issue authentication failure traps.
- **link-up-down** - Keyword to issue link-up or link-down traps.

Default Setting

Issue all traps.

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.
- The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.
- The notification types used in this command all have an associated MIB object that allows them to be globally enabled or disabled. Not all of the notification types have notificationEnable MIB objects, so some of these cannot be controlled using the **snmp-server enable traps** command.

Example

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Related Commands

snmp-server host

---

snmp ip filter

Sets the IP addresses of clients that are allowed management access to the switch via SNMP. Use the no form of this command to remove an IP address.

Syntax

snmp ip filter *ip_address subnet_mask*
no snmp ip filter *ip_address subnet_mask*

- *ip_address* - An IP address indicating a client or group of clients that are allowed SNMP access to the switch.
- *subnet_mask* - An address bitmask of decimal numbers that represent the address bits to match.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- You can create a list of up to 16 IP addresses or IP address groups that are allowed access to the switch via SNMP management software.
- Address bitmasks are similar to a subnet mask, containing four decimal integers from 0 to 255, each separated by a period. The binary mask uses “1” bits to indicate “match” and “0” bits to indicate “ignore.”
- If the IP is the address of a single management station, the bitmask should be set to 255.255.255.255. Otherwise, the IP address group is specified by the bitmask.
- The default setting is null, which allows all IP groups SNMP access to the switch. If one IP address is configured, the IP filtering is enabled and only addresses in the IP group will have SNMP access.
- IP filtering does not affect management access to the switch using the Web interface or Telnet.

Example

The following example enables SNMP IP filtering on the switch and allows SNMP management access to client IP 10.1.2.3, and client IP group 10.1.3.0 to 10.1.3.255.

```
Console(config)#snmp ip filter 10.1.2.3 255.255.255.255
Console(config)#snmp ip filter 10.1.3.0 255.255.255.0
Console(config)#
```

Related Commands

show snmp

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

IGMP Snooping Commands:
Dell PowerConnect Switch User's Guide

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

---

ip igmp snooping

Use this command to enable IGMP snooping on this switch. Use the **no** form to disable it.

Command Syntax

ip igmp snooping
no ip igmp snooping

Default Setting

Enabled

Command Mode

Global Configuration

Example

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

---

ip igmp snooping vlan mrouter

Use this command to statically configure a multicast router port. Use the **no** form to remove the configuration.

Command Syntax

ip igmp snooping vlan *vlan-id* **mrouter** *interface*
no ip igmp snooping vlan *vlan-id* **mrouter** *interface*

- *vlan-id* - VLAN ID (1-4094)
- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your switch, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

---

ip igmp snooping vlan static

Use this command to add a port to a multicast group. Use the **no** form to remove the port.

Command Syntax

ip igmp snooping vlan *vlan-id* **static** *ip-address interface*
no ip igmp snooping vlan *vlan-id* **static** *ip-address interface*

- *vlan-id* - VLAN ID (Range: 1-4094)
- *ip-address* - IP address for multicast group
- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- The maximum number of IGMP multicast group entries -
  - PowerConnect 3248: 64
  - PowerConnect 5224: 64

Example

The following shows how to statically configure a multicast group on a port:

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

---

ip igmp snooping querier

Use this command to enable the switch as an IGMP snooping querier. Use the **no** form to disable it.

Command Syntax

ip igmp snooping querier
no ip igmp snooping querier

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

---

ip igmp snooping query-count

Use this command to configure the query count. Use the **no** form to restore the default.

Command Syntax

ip igmp snooping query-count *count*
no ip igmp snooping query-count

count - The maximum number of queries issued for which there has been no response before the switch takes action to solicit reports. (Range: 2-10)

Default Setting

2 times

Command Mode

Global Configuration

Command Usage

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by **ip igmp snooping query-max- response-time**. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

---

ip igmp snooping query-interval

Use this command to configure the snooping query interval. Use the **no** form to restore the default.

Command Syntax

ip igmp snooping query-interval *seconds*
no ip igmp snooping query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 60-125)

Default Setting

125 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

---

ip igmp snooping query-max-response-time

Use this command to configure the snooping report delay. Use the **no** form of this command to restore the default.

Command Syntax

ip igmp snooping query-max-response-time *seconds*
no ip igmp snooping query-max-response-time

seconds - The report delay advertised in IGMP queries. (Range: 5-30)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the **ip igmp snooping query-count**, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

Related Commands

ip igmp snooping version

---

ip igmp snooping query-time-out

Use this command to configure the snooping query-timeout. Use the **no** form of this command to restore the default.

Command Syntax

ip igmp snooping query-time-out *seconds*
no ip igmp snooping query-time-out

seconds - The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The switch must be using IGMPv2 for this command to take effect.

Example

The following shows how to configure the default timeout to 300 seconds:

```
Console(config)#ip igmp snooping query-time-out 300
Console(config)#
```

Related Commands

ip igmp snooping version

---

ip igmp snooping version

Use this command to configure the IGMP snooping version. Use the **no** form to restore the default.

Command Syntax

ip igmp snooping version {**1** | **2**}
no ip igmp snooping version

- **1** - IGMP Version 1
- **2** - IGMP Version 2

Default Setting

IGMP Version 2

Command Mode

Global Configuration

Command Usage

- All systems on the subnet must support the same version. If there are legacy devices in your network that only support Version 1, you will also have to configure this switch to use Version 1.
- Some commands are only enabled for IGMPv2, including **ip igmp query-max-response-time** and **ip igmp query-timeout**.

Example

The following configures the switch to use IGMP Version 1:

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

---

show ip igmp snooping

Use this command to show the IGMP snooping configuration.

Default Setting

None

Command Mode

Privileged Exec

Example

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
 Service status: Enabled
 Querier status: Enabled
 Query count: 2
 Query interval: 125 sec
 Query max response time: 10 sec
 Query time-out: 300 sec
 IGMP snooping version: Version 2
Console#
```

---

show ip igmp snooping mrouter

Use this command to display information on statically configured and dynamically learned multicast router ports.

Command Syntax

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static or Dynamic.

Example

The following shows the ports in VLAN 1 which are attached to multicast routers:

```
Console#show ip igmp snooping mrouter vlan 1
VLAN M'cast Router Port Type
---- ------------------ -------
```

```
   1           Eth 1/11  Static
   2           Eth 1/12 Dynamic
Console#
```

---

show mac-address-table multicast

Use this command to show the multicast list with MAC and IP addresses.

Command Syntax

show mac-address-table multicast [**vlan** *vlan-id*] [**user** | **igmp-snooping**]

- *vlan-id* - VLAN ID (1 to 4094)
- **user** - Display only the user-configured multicast entries.
- **igmp-snooping** - Display only entries learned through IGMP snooping.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Member types displayed include IGMP or USER, depending on selected options.
- The maximum number of IGMP multicast group entries -
  - PowerConnect 3248: 64
  - PowerConnect 5224: 64

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1       224.1.2.3      Eth1/11    User
Console#
```

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

Spanning Tree Commands:
Dell PowerConnect Switch User's Guide

These commands are used to configure STP for the overall switch, or to configure STP for the selected interface.

---

spanning-tree

Use this command to enable the Spanning Tree Protocol globally for the switch. Use the **no** form to disable it.

Syntax

spanning-tree
no spanning-tree

Default Setting

Spanning Tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Protocol can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

The following example shows how to enable the Spanning Tree Protocol for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

---

spanning-tree mode

Use this command to select the Spanning Tree mode for the switch. Use the **no** form to restore the default.

Syntax

spanning-tree mode {**stp** | **rstp**}
no spanning-tree mode

- **stp** - Spanning Tree Protocol (IEEE 802.1D)
- **rstp** - Rapid Spanning Tree (IEEE 802.1w)

Default Setting

rstp

Command Mode

Global Configuration

Command Usage

- Spanning Tree Protocol

STP creates one Spanning Tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members.

- Rapid Spanning Tree Protocol
  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:
  - STP Mode - If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
  - RSTP Mode - If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

Example

The following example configures the switch to use Rapid Spanning Tree.

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

---

spanning-tree forward-time

Use this command to configure the Spanning Tree bridge forward time globally for the switch. Use the **no** form to restore the default.

Syntax

spanning-tree forward-time *seconds*
no spanning-tree forward-time

seconds - Time in seconds. (Range: 4 - 30 seconds)
The minimum value is the higher of 4 or [(**max-age** / 2) + 1].

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

---

spanning-tree hello-time

Use this command to configure the Spanning Tree bridge hello time globally for the switch. Use the **no** form to restore the default.

Syntax

spanning-tree hello-time *time*
no spanning-tree hello-time

time - Time in seconds. (Range: 1 - 10 seconds)
The maximum value is the lower of 10 or [(**max-age** / 2) -1].

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
```

```
Console(config)#
```

spanning-tree max-age

Use this command to configure the Spanning Ttree bridge maximum age globally for the switch. Use the **no** form to restore the default.

Syntax

spanning-tree max-age *seconds*
no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)
The minimum value is the higher of 6 or [2 x (hello-time + 1)].
The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

spanning-tree priority

Use this command to configure the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree priority *priority*
no spanning-tree priority

priority - Priority of the bridge.
(Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

spanning-tree pathcost method

Use this command to configure the path cost method used for the Rapid Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree pathcost method {**long** | **short**}

no spanning-tree pathcost method

- **long** - Specifies 32-bit based values that range from 1-200,000,000.
- **short** - Specifies 16-bit based values that range from 1-65535.

Default Setting

short method

Command Mode

Global Configuration

Command Usage

The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost takes precedence over port priority.

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

---

spanning-tree transmission-limit

Use this command to configure the minimum interval between the transmission of consecutive RSTP BPDUs. Use the **no** form to restore the default.

Syntax

spanning-tree transmission-limit *count*
no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

Default Setting

3

Command Mode

Global Configuration

Command Usage

This command limit the maximum transmission rate for BPDUs.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

---

spanning-tree cost

Use this command to configure the spanning tree path cost for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree cost *cost*
no spanning-tree cost

- *cost* - The path cost for the interface.
  (Range - 1-200,000,000)
  The recommended range is -
  - Ethernet: 200,000-20,000,000
  - Fast Ethernet: 20,000-2,000,000
  - Gigabit Ethernet: 2,000-200,000

Default Setting

- Ethernet - half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet - half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet - full duplex: 10,000; trunk: 5,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used by the Spanning-Tree Protocol to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.
- Path cost takes precedence over interface priority.
- When the Spanning-Tree pathcost method is set to **short**, the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

Related Commands

spanning-tree port-priority

---

spanning-tree port-priority

Use this command to configure the priority for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree port-priority *priority*
no spanning-tree port-priority

priority - The priority for an interface. (Range: 0-240, in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of an interface in the Spanning-Tree. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the Spanning Tree.
- Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#
```

Related Commands

spanning-tree cost

---

spanning-tree portfast

Use this command to set an interface to fast forwarding. Use the **no** form to disable fast forwarding.

Syntax

spanning-tree portfast
no spanning-tree portfast

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used to enable/disable the fast Spanning-Tree mode for the selected interface. In this mode, interfaces skip the Learning state and proceed straight to Forwarding.
- Since end-nodes cannot cause forwarding loops, they can be passed through the Spanning Tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STP related timeout problems. (Remember that fast forwarding should only be enabled for interfaces connected to an end-node device.)
- This command has the same effect as the **spanning-tree edge-port** command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree portfast
Console(config-if)#
```

Related Commands

spanning-tree edge-port

---

spanning-tree edge-port

Use this command to specify an interface as an edge port. Use the **no** form to restore the default.

Syntax

spanning-tree edge-port
no spanning-tree edge-port

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- You can enable this option if an interface is attached to a LAN segment that is at the end of bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the Spanning Tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the Spanning Tree to initiate reconfiguration when the interface changes state, and also overcomes other STP-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- This command has the same effect as the **spanning-tree portfast** command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

Related Commands

spanning-tree portfast

---

spanning-tree link-type

Use this command to configure the link type for the Rapid Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree link-type {**auto** | **point-to-point** | **shared**}
no spanning-tree link-type

- **auto** - Automatically derived from the duplex mode setting.
- **point-to-point** - Point-to-point link.
- **shared** - Shared medium.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
Console(config-if)#
```

---

spanning-tree protocol-migration

Use this command to re-check the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

interface

- **ethernet** *unit/port-number*
  - *unit* - This is device 1.
  - *port-number*
- **port-channel** *channel-id* (Range: 1-6)

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree protocol-migration
Console(config-if)#
```

---

show spanning-tree

Use this command to show the Spanning Tree configuration.

Syntax

show spanning-tree [*interface*]

interface
- **ethernet** *unit/port-number*
  - *unit* - This is device 1.
  - *port-number* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use the **show spanning-tree** command with no parameters to display the configuration for the Spanning Tree and for every interface in the tree.
- Use the **show spanning-tree** *interface* command to display the Spanning Tree configuration for an interface within the Spanning Tree.

Example

```
Console#show spanning-tree
```

```
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode                :RSTP
 Spanning tree enable/disable      :enable
 Priority                          :32768
 Bridge Hello Time (sec.)          :2
 Bridge Max Age (sec.)             :20
 Bridge Forward Delay (sec.)       :15
 Root Hello Time (sec.)            :2
 Root Max Age (sec.)               :20
 Root Forward Delay (sec.)         :15
 Designated Root                   :32768.000011112222
 Current root port                 :0
 Current root cost                 :0
 Number of topology changes        :1
 Last topology changes time (sec.):25067
 Transmission limit                :3
 Path Cost Method                  :long
---------------------------------------------------------------
Eth 1/ 1 information
---------------------------------------------------------------
 Admin status          : enable
 Role                  : disable
 State                 : discarding
 Path cost             : 10000
 Priority              : 128
 Designated cost       : 0
 Designated port       : 128.1
 Designated root       : 32768.000011112222
 Designated bridge     : 32768.000011112222
 Fast forwarding       : disable
 Forward transitions   : 0
 Admin edge port       : disable
 Oper edge port        : disable
 Admin Link type       : auto
 Oper Link type        : point-to-point
.
.
.
Console#
```

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

System Management Commands:
Dell PowerConnect Switch User's Guide

These commands are used to control system logs, passwords, user name, browser configuration options, and display or configure a variety of other system information.

---

enable password

After initially logging onto the system, you should set the administrator (Privileged Exec) and guest (Normal Exec) passwords. Remember to record them in a safe place. Use the **enable password** command to set the password for access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

enable password [**level** *level*] {**0** | **7**} *password*
no enable password [**level** *level*]

- **level** *level* - Only level **15** (Privileged Exec) is valid for this command.
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- *password* - password for this privilege level.
  (Maximum length: 8 characters, case sensitive)

Default Setting

The default password is "super"

Command Mode

Global Configuration

Command Usage

- You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the enable command.
- The encrypted password is required for compatiblity with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

enable

---

logging on

Use this command to control logging of error messages. This command sends debug or error messages to a logging process. The **no** form disables the logging process.

Syntax

logging on
no logging on

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to switch memory or sent to remote syslog servers. You can use the **logging history** command to control the type of error messages that are stored in memory. The **logging trap** command controls the type of error messages that are sent to specified syslog servers.

Example

```
Console(config)#logging on
Console(config)#
```

Related Commands

logging history
logging trap
clear logging

---

logging history

Use this command to limit syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

Syntax

logging history {**flash** | **ram**} *level*
no logging history {**flash** | **ram**}

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- *level* - One of the level arguments listed in Table 1. Messages sent include the selected level up through level 0.

Table 1. Message Levels

Level Argument	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Default Setting

Flash: errors (level 3 - 0)
RAM: warnings (level 7 - 0)

Command Mode

Global Configuration

Command Usage

- The message level specified for Flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.
- The switch can hold up to 4096 event log entries in Flash memory, with the oldest entries being overwritten first when the available memory for logs (256 Kilobyte) has been exceeded.

Example

```
Console(config)#logging history ram 0
Console(config)#
```

Related Commands

- logging host
- logging trap

---

logging host

Use this command to add a syslog server host IP address that will receive logging messages. Use the **no** form to remove a syslog server host.

Syntax

logging host *host_ip_address*
no logging host *host_ip_address*

host_ip_address - The IP address of a syslog server.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- By using this command more than once you can build up a list of host IP addresses.
- The maximum number of host IP addresses allowed is five.

Example

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

Related Commands

logging history
logging trap

---

logging facility

Use this command to set the facility type for remote logging of syslog messages. Use the **no** form to return the type to the default.

Syntax

logging facility *type*
no logging facility *type*

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default Setting

23

Command Mode

Global Configuration

Example

```
Console(config)#logging facility 19
Console(config)#
```

Related Commands

logging history
logging trap

---

logging trap

Use this command to limit syslog messages saved to a remote server based on severity. Use the **no** form to return the remote logging of syslog messages to the default level.

Syntax

logging trap *level*
no logging trap *level*

level - One of the level arguments listed in Table 1 above. Messages sent include the selected level up through level 0.

Default Setting

Level 3 - 0

Command Mode

Global Configuration

Example

```
Console(config)#logging trap 4
Console(config)#
```

Related Commands

logging history
logging host

---

clear logging

Use this command to clear messages from the log buffer.

Syntax

clear logging [**flash** | **ram**]

- **flash** - Event history stored in Flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear logging
Console#
```

Related Commands

show logging

---

username

Use this command to require user name authentication at login. Use the **no** form to remove a user name.

Syntax

username *name* {**access-level** *level* | **nopassword** | **password** {**0 | 7**} *password*}
no username *name*

- *name* - The name of the user.
  (Maximum length: 8 characters, case sensitive; maximum number of users: 16)
- **access-level** *level* - Specifies the user level.
  The device has two predefined privilege levels: **0**: Normal Exec, **15**: Privileged Exec.
- **nopassword** - No password is required for this user to log in.
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- **password** *password* - The authentication password for the user.

(Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default access level is Normal Exec.
- Factory defaults for the user names and passwords are:

username	**access-level**	**password**
guest admin	0 (Normal Exec) 15 (Privileged Exec)	guest admin

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatiblity with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

---

hostname

Use this command to specify or modify the host name for this device. Use the **no** form to restore the default host name.

Syntax

hostname *name*
no hostname

name - The name of this host. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#hostname Server Chassis 35
Console(config)#
```

---

jumbo frame

Use this command to enable jumbo frames through this device. Use the **no** form to disable jumbo frames.

Syntax

jumbo frame
no jumbo frame

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- This command is only available for the PowerConnect 5224.
- This switch provides more efficient throughput for large sequential data transfers by supporting Jumbo frames up to 9000 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

- To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.
- Enabling jumbo frames will limit the maximum threshold for broadcast storm control to 64 packets per second. (See the switchport broadcast command.)

Example

```
Console(config)#jumbo frame
Console(config)#
```

---

ip http port

Use this command to specify the TCP port number used by the Web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*
no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 1-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
Console(config)#ip http port 769
Console(config)#
```

Related Commands

ip http server

---

ip http server

Use this command to allow this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

ip http server
no ip http server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip http server
Console(config)#
```

Related Commands

ip http port

---

ip http secure-port

Use this command to specify the UDP port number used for HTTPS/SSL connection to the switch's Web interface. Use the **no** form to restore the default port..

Syntax

ip http secure-port *port-number*
no ip http secure-port

port-number - The UDP port used for HTTPS/SSL. (Range: 1-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- You cannot configure the HTTP and HTTPS servers to use the same port.
- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: **https:**//*device:port_number*

Example

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

ip http secure-server

---

ip http secure-server

Use this command to enable the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's Web interface. Use the **no** form to disable this function.

Syntax

ip http secure-server
no ip http secure-server

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- Both HTTP and HTTPS service can be enabled independently.
- If you enable HTTPS, you must indicate this in the URL: **https:**//*device*[*port_number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection. A padlock icon should appear in the status bar for Internet Explorer 5.x and Netscape Navigator 4.x.
- The following Web browsers and operating systems currently support HTTPS:

Table 2. Web Browsers

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000
Netscape Navigator 4.76 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Solaris 2.6

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

ip http secure-port
copy tftp https-certificate

---

ip ssh server

Use this command to enable the Secure Shell (SSH) server on this switch. Use the **no** form to disable this service.

Syntax

ip ssh server
no ip ssh server

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- The SSH server uses RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

Example

```
Console(config)#ip ssh server
Console(config)#
```

Related Commands

show ssh

---

ip ssh

Use this command to configure authentication control parameters for the Secure Shell (SSH) server on this switch. Use the **no** form to restore the default settings.

Syntax

ip ssh {[**timeout** *seconds*] | [**authentication-retries** *count*]}
no ip ssh {[**timeout**] | [**authentication-retries**]}

seconds – The timeout for client response during SSH negotiation. (Range: 1-120)
count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Setting

Timeout: 120 seconds
Count: 3

Command Mode

Global Configuration

Command Usage

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the **exec-timeout** command for vty sessions.

Example

```
Console(config)#ip ssh timeout 60
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

Related Commands

show ip ssh

---

disconnect ssh

Use this command to terminate a Secure Shell (SSH) client connection.

Syntax

disconnect ssh *connection-id*

connection-id – The session identifier as displayed in the **show ip ssh** command.

Command Mode

Privileged Exec

Example

```
Console#disconnect ssh 0
Console#
```

Related Commands

show ip ssh

---

show startup-config

Use this command to display the configuration file stored in non-volatile memory that is used to start up the system.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show startup-config
building startup-config, please wait.....
!
hostname Switch
snmp-server location Boston
snmp-server contact Charles
!
snmp-server community private rw
snmp-server community public ro
!
no snmp-server enable traps authentication
username guest access-level 0
username guest password guest
username admin access-level 15
username admin password admin
enable password level 0 0 guest
enable password level 15 0 admin
no logging on
!
vlan database
vlan 1 name DefaultVlan media ethernet state active
!
interface ethernet 1/1
no capabilities flowcontrol
switchport allowed vlan add 1 untagged
switchport native vlan 1.
.
.
.
interface vlan 1
ip address 10.1.0.1 255.255.255.0
!
no bridge 1 spanning-tree
!
line console
!
line vty
!
end
Console#
```

Related Commands

show running-config

---

show running-config

Use this command to display the configuration information currently in use.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.

Example

```
Console#show running-config
building running-config, please wait.....
!
!
snmp-server community private rw
snmp-server community public ro
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
.
.
.
interface vlan 1
ip address 10.1.0.4 255.255.255.0
!
!
!
!
!
!
!
line console
!
!
line vty
exec-timeout 65535
!
!
!
end
Console#
```

Related Commands

show startup-config

---

show logging

Use this command to display the logging configuration for system and event messages.

Syntax

show logging {**flash** | **ram | trap**}

- **flash** - Event history stored in Flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- **trap** - Messages sent to remote syslog servers.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show logging flash
Syslog logging: Disable
History logging in FLASH: level errors
Console#show logging trap
Syslog logging: Enable
REMOTELOG status: enable
REMOTELOG facility type: local use 3
REMOTELOG level type: Warning conditions
REMOTELOG server ip address: 10.1.0.3
REMOTELOG server ip address: 10.1.0.4
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
[3] 0:0:41 1/1/1
   "VLAN 1 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[2] 0:0:41 1/1/1
   "STA topology change notification."
   level: 6, module: 6, function: 1, and event no.: 1
[1] 0:0:12 1/1/1
   "Unit 1, Port 5 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[0] 0:0:11 1/1/1
   "System coldStart notification."
   level: 6, module: 6, function: 1, and event no.: 1
Console#
```

---

show system

Use this command to display system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show system
System description: PowerConnect 3248
System OID string: 1.3.6.1.4.1.674.10895.3
System information
 System Up time: 0 days, 0 hours, 55 minutes, and 54.91 seconds
 System Name            : Switch
 System Location        : Boston
 System Contact         : Charles
 MAC address            : 00-00-e8-00-00-01
 Web server             : enable
 Web server port        : 80
 Web secure server      : enable
 Web secure server port : 443
 POST result
UART Loopback Test......................PASS
Timer Test..............................PASS
DRAM Test ..............................PASS
I2C Initialization......................PASS
Runtime Image Check ....................PASS
PCI Device Check .......................PASS
Switch Driver Initialization............PASS
Switch Internal Loopback Test...........PASS
------------------- DONE --------------------
Console#
```

---

show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show users
 Username accounts:
  Username Privilege
  -------- ---------
     guest         0
     admin        15

 Online users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
  0   console    admin           0:04:37
* 1     vty 0    admin           0:00:00         0.0.0.0

Console#
```

---

show version

Use this command to display hardware and software version information for the system.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show version
Unit1
Serial number          :0000000000000000000
Service tag            :0000000
Hardware version       :R0C
Number of ports        :50
Main power status      :up
Redundant power status :not present
Agent(master)
Unit id                :1
Loader version         :1.0.0.0
Boot rom version       :1.0.0.3
Operation code version :2.0.0.19
Console#
```

---

show ip ssh

Use this command to display the connection settings used when authenticating client access to the Secure Shell (SSH) server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
Information of secure shell
SSH status: enable
SSH authentication timeout: 120
SSH authentication retries: 3
Console#
```

Related Commands

ip ssh

---

show ssh

Use this command to display the current Secure Shell (SSH) server connections.

Command Mode

Privileged Exec

Command Usage

This command shows the following information:

- **Session** - The session number. (Range: 0-3)
- **Username** - The user name of the client.
- **Version** - The Secure Shell version number.
- **Encrypt method** - The encryption method. (Options: cipher-des, cipher-3des)
- **Negotiation state** - The authentication negotiation state.

Example

```
Console#show ssh
Information of secure shell
Session Username Version Encrypt method Negotiation state
------- -------- ------- -------------- -----------------
      0    admin     1.5    cipher-3des   session-started
Console#
```

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

Time Commands:
Dell PowerConnect Switch User's Guide

These commands are used to set and display the system clock.

---

calendar set

Use this command to set the system clock.

Syntax

calendar set *hour:min:sec* {*day month year* | *month day year*}

- *hour:min:sec* - Hour (24-hour format), minute, second.
- *day* - Day of month.
- *month* - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**
- *year* - Year (4-digit).

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows how to set the system clock to 15:12:34, February 1st, 2002.

```
Console# calendar set 15:12:34 1 February 2002
Console#
```

---

show calendar

Use this command to display the system clock.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

This example shows how to set the system clock set at 15:12:34, February 1st, 2002.

```
Console# show calendar set
15:12:34 1 February 2002
Console#
```

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

Port Trunking Commands:
Dell PowerConnect Switch User's Guide

Ports can be statically grouped into an aggregate link to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to be compatible with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to six trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

---

channel-group

Use this command to add a port to a trunk. Use the **no** form to remove a port from a trunk.

Command Syntax

channel-group *channel-id*
no channel-group

channel-id - Trunk index (Range: 1-6)

Default Setting

A new trunk contains no ports.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When configuring static trunks, the switches must be compatible with the Cisco EtherChannel standard.
- Use **no channel-group** to remove a port group from a trunk.
- Use **no interfaces port-channel** to remove a trunk from the switch.
- The maximum number of ports that can be combined as a static trunk - PowerConnect 3248: 4 10/100 Mbps ports, 2 1000 Mbps ports; PowerConnect 5224: 6 1000 Mbps ports.
- All links in a trunk group must operate at the same data rate and duplex mode.

Example

The following example creates trunk 1 and then adds port 11:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

Please read all restrictions and disclaimers.

Back to Contents Page

Back to Contents Page

VLAN Commands:
Dell PowerConnect Switch User's Guide

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

---

vlan database

Use this command to enter VLAN database mode. All commands in this mode will take effect immediately.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the **show vlan** command.
- Use the **interface vlan** command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the **show running-config** command.

Example

```
Console(config)#vlan database
Console(config-vlan)#
```

Related Commands

show vlan

---

vlan

Use this command to configure a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**suspend** | **active**}]
no vlan *vlan-id* [**name** | **state**]

- *vlan-id* - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  - *vlan-name* - ASCII string 1 to 32 characters.
- **media ethernet** - Ethernet media type.
- **state** - Keyword to be followed by the VLAN state.
  - **active** - VLAN is operational.
  - **suspend** - VLAN is suspended. Suspended VLANs do not pass packets.

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- When **no vlan** *vlan-id* is used, the VLAN is deleted.
- When **no vlan** *vlan-id* **name** is used, the VLAN name is removed.
- When **no vlan** *vlan-id* **state** is used, the VLAN returns to the default state (i.e., active).
- VLAN 1 cannot be suspended, but any other VLAN can be suspended.
- You can configure up to 255 VLANs on this switch.

Example

The following example adds a VLAN, using vlan-id 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

show vlan

---

interface vlan

Use this command to enter interface configuration mode for VLANs, and configure a physical interface.

Syntax

interface vlan *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)

Default Setting

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

shutdown

---

switchport ingress-filtering

Use this command to enable ingress filtering for an interface. Use the **no** form to restore the default.

Syntax

switchport ingress-filtering
no switchport ingress-filtering

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Ingress filtering only affects tagged frames.

- If ingress filtering is disabled, the interface will accept any VLAN-tagged frame if the tag matches a VLAN known to the switch (except for VLANs explicitly forbidden on this port).
- If ingress filtering is enabled, incoming frames tagged for VLANs which do not include this ingress port in their member set will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

---

switchport acceptable-frame-types

Use this command to configure the acceptable frame types for a port. Use the **no** form to restore the default.

Syntax

switchport acceptable-frame-types {**all** | **tagged**}
no switchport acceptable-frame-types

- **all** - The port passes all frames, tagged or untagged.
- **tagged** - The port only passes tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following example shows how to restrict the traffic passed on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

Related Commands

switchport mode

---

switchport mode

Use the **switchport mode** command to configure the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {**trunk** | **hybrid**}
no switchport mode

- *trunk* - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits and receives tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are sent untagged.
- *hybrid* - Keyword that specifies a hybrid VLAN interface. The port may receive or transmit tagged or untagged frames.

Default Setting

All ports are in hybrid mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to **hybrid**:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

Related Commands

switchport acceptable-frame-types

---

switchport gvrp

Use this command to enable GVRP for a port. Use the **no** form to disable it.

Syntax

switchport gvrp
no switchport gvrp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

---

switchport allowed vlan

Use this command to configure VLAN groups on the selected interface. Use the **no** form to restore the default.

Syntax

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] | **remove** *vlan-list*}
no switchport allowed vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094)

Default Setting

All ports are assigned to VLAN 1 by default.
The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If switchport mode is set to **trunk**, then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 2,5,6 tagged
Console(config-if)#
```

---

switchport native vlan

Use this command to configure the PVID (i.e., default VID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*
no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4094, no leading zeroes)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

---

switchport forbidden vlan

Use this command to configure forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

Syntax

switchport forbidden vlan {**add** *vlan-id* | **remove** *vlan-id*}
no switchport forbidden vlan

- **add** *vlan-id* - VLAN ID to add.
- **remove** *vlan-id* - VLAN ID to remove.

(Range: 1-4094, no leading zeroes)

Default Setting

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

Example

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

---

show vlan

Use this command to show VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- **name** - Keyword to be followed by the VLAN ID.
  - *vlan-id* - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  - *vlan-name* - ASCII string 1 to 32 characters.

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows how to display information for VLAN 1:

```
Console#show vlan id 1
VLAN Type    Name             Status    Ports/Channel groups
---- ------- ---------------- --------- --------------------------------------
   1  Static      DefaultVlan    Active Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4 Eth1/ 5
                                        Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9 Eth1/10
                                        Eth1/11 Eth1/12 Eth1/13 Eth1/14 Eth1/15
                                        Eth1/16 Eth1/17 Eth1/18 Eth1/19 Eth1/20
                                        Eth1/21 Eth1/22 Eth1/23 Eth1/24
Console#
```

Please read all restrictions and disclaimers.

Back to Contents Page