Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

Using the CLI
Command Groups
AAA Commands
Address Table Commands
Ethernet Configuration Commands
Configuration and Image Files
IGMP Snooping Commands
GVRP Commands
IP Addressing Commands
LACP Commands
Line Commands
Management ACL
Port Channel Commands
Port Monitor Commands
QoS Commands
Radius Commands
RMON Commands
SNMP Commands
Spanning Tree Commands
SSH Commands
Syslog Commands
System Management
User Interface Commands
VLAN Commands
Web Server

Models 3324 and 3348

Notes, Notices, and Cautions

NOTE: A NOTE indicates important information that helps you make better use of your computer.

NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

CAUTION: A CAUTION indicates a potential for property damage, personal injury, or death.

May 2003 P/N J0926 Rev. A00

Back to Contents Page

AAA Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- aaa authentication login
- aaa authentication enable
- login authentication
- enable authentication
- ip http authentication
- ip https authentication
- show authentication methods
- password
- enable password
- username
- show users accounts

---

aaa authentication login

Use the **aaa authentication login** global configuration command to define login authentication. To return to the default configuration, use the **no** form of this command.

Syntax

aaa authentication login {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication login {**default** | *list-name*}

- **default**—Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
- *list-name*—Character string used to name the list of authentication methods activated when a user logs in.
- *method1* [*method2*...]—Select at least one method from the following table:

Keyword	Source or destination
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local user name database for authentication.
none	Uses no authentication. Access can be provided without authorization if defined as a specific authentication method.
radius	Uses the list of all RADIUS servers for authentication.

Default Configuration

The local user database is checked. This has the same effect as the **aaa authentication login local** command.

NOTE: On the console, login succeeds without any authentication check if the authentication method is not defined.

Command Mode

Global Configuration Mode

User Guidelines

The default and optional list names created with the **aaa authentication login** command are used with the **login authentication** command.

Use the **aaa authentication login** *list-name method* command to creat a list for a particular protocol, where *list-name* is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

The following is an example of the CLI commands.

```
Console (config)# aaa authentication login default radius local enable none
```

---

aaa authentication enable

Use the **aaa authentication enable default** global configuration command to define authentication method lists for accessing higher privilege levels. To return to the default configuration, use the **no** form of this command.

Syntax

aaa authentication enable {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication enable default

- **default**—Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
- *list-name*—Character string used to name the list of authentication methods activated, when using access higher privilege levels.
- *method1* [*method2*...]—Select at least one method from the following table:

Keyword	Source or destination
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication. Access can be provided without authorization if defined as a specific authentication method.
radius	Uses the list of all RADIUS servers for authentication. Uses user name **$enabx$.** where x is the privilege level.

Default Configuration

If the **default** list is not set, only the enable password is checked. This has the same effect as the **aaa authentication enable default enable** command.

On the console, the enable password is used if it exists. If no password is set, the process still succeeds. This has the same effect as using the **aaa authentication enable default enable none** command.

Command Mode

Global Configuration Mode

User Guidelines

The default and optional list names created with the **aaa authentication enable** command are used with the **enable authentication** command.

Use the **aaa authentication enable** *list-name method* command to create a list, where *list-name* is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

All **aaa authentication enable default** requests sent by the device to a RADIUS server include the username **$enab***x***$.**, where *x* is the requested privilege level.

Example

The following example sets authentication when accessing higher privilege levels.

```
Console (config)# aaa authentication enable default
```

---

login authentication

Use the **login authentication** line configuration command to specify the login authentication method list for a remote Telnet or console. To return to the default specified by the **authentication login** command, use the **no** form of this command.

Syntax

login authentication {**default** | *list-name*}

no login authentication

- **default**—Uses the default list created with the **authentication login** command.
- *list-name*—Uses the indicated list created with the **authentication login** command.

Default Configuration

Uses the default set with the command **authentication login**.

Command Mode

Line Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the default authenticationmethod for a remote Telnet or console.

```
Console (config-line)# login authentication default
```

---

enable authentication

Use the **enable authentication** line configuration command to specify the authentication method list when accessing a higher privilege level from a remote Telnet or console. To return to the default specified by the **enable authentication** command, use the **no** form of this command.

Syntax

enable authentication {**default** | *list-name*}

no enable authentication

- **default**—Uses the default list created with the **authentication enable** command.
- *list-name*—Uses the indicated list created with the **authentication enable** command.

Default Configuration

Uses the default set with the **authentication enable** command.

Command Mode

Line Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the default authentication method when accessing a higher privilege level from a remote Telnet or console.

```
Console (config-line)# enable authentication default
```

---

ip http authentication

Use the **ip http authentication** global configuration mode command to specify authentication methods for http. To return to the default, use the **no** form of this command.

Syntax

ip http authentication *method1* [*method2*...]

no ip http authentication

- *method1* [*method2*...]—Select at least one method from the following table:

Keyword	Source or destination
local	Uses the local user name database for authentication.
none	Uses no authentication. Access can be provided without authorization if defined as a specific authentication method.
radius	Uses the list of all RADIUS servers for authentication.

Default Configuration

The local user database is checked. This has the same effect as the **ip http authentication local** command.

Command Mode

Global Configuration Mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method from the command line.

Example

The following example configures the http authentication as either RADIUS or local in that order.

```
Console (config)# ip http authentication radius local
```

---

ip https authentication

Use the **ip https authentication** global configuration command to specify authentication methods for https. To return to the default, use the **no** form of this command.

Syntax

ip https authentication *method1* [*method2*...]

no ip https authentication

- *method1* [*method2*...]—Select at least one method from the following table:

Keyword	Source or destination
local	Uses the local user name database for authentication.
none	Uses no authentication. Access can be provided without authorization if defined as a specific authentication method.
radius	Uses the list of all RADIUS servers for authentication.

Default Configuration

The local user database is checked. This has the same effect as the **ip https authentication local** command.

Command Mode

Global Configuration Mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

Example

The following is an example of the CLI command.

```
Console (config)# ip https authentication radius local
```

---

show authentication methods

Use the **authentication methods** privilege EXEC command to display information about the authentication methods.

Syntax

show authentication methods

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the authentication configuration.

```
Console# show authentication methods


Login Authentication Method Lists

---------------------------------

Default: Radius, Local, Line

Console_Login: Line, None


Enable Authentication Method Lists

---------------------------------

Default: Radius, Enable

Console_Enable: Enable, None




Line Login Method List Enable Method List

------- ----------------- -------------------
```

```
Console Console_Login Console_Enable


Telnet Default Default


SSH Default Default



HTTP: Radius, local


HTTPS: Radius, local
```

---

password

Use the **password** line configuration command to specify a password on a command line. To remove the password, use the **no** form of this command.

Syntax

password *password* [**encrypted**]

no password

- *password*—Password for this level, from 1 to 159 characters in length.
- **encrypted**—Encrypted password to be entered, copied from another device configuration.

Default Configuration

This command has no default configuration.

Command Mode

Line Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies a password.

```
Console (config-line)# password dell
```

enable password

Use the **enable password** global configuration command to set a local password to control access to user and privilege levels. To remove the password requirement, use the **no** form of this command.

Syntax

enable password [**level** *level*] *password* [**encrypted**]

no enable password [**level** *level*]

- *password*—Password for this level, from 1 to 159 characters in length.
- **level** *level*—Level for which the password applies. If not specified, the level is **15** (Range: **1-15**).
- **encrypted**—Encrypted password entered, copied from another device configuration.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets a local level for a password to control access to user and privilege levels.

```
Console (config)# enable password level 15 dell
```

username

Use the **username** global configuration command to establish a user name-based authentication system. To remove a user name, use the **no** form of this command.

Syntax

username *name* [**password** *password*] [*privilege level*] [**encrypted**]

no username

- *name*—The user name.
- *password*—The user authentication password (Range: **1-159**).
- *privilege level*—Specifies the user level (Range: **1-15**).
- **encrypted**—Encrypted password entered, copied from another device configuration.

Default Configuration

The default privilege level is **1**.

Command Mode

Global Configuration Mode

User Guidelines

When creating a user name, the default priority is **1**, which does not allow access to the device. A priority of **15** must be specifically set to enable access to the device.

Example

The following example configures a user with the encrypted password and user level for the system.

```
Console (config)# username bob password lee 15 encrypted
```

---

show users accounts

The **show users accounts** privileged EXEC command displays information about the local user database.

Syntax

show users accounts

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the local users configured with access to the system.

```
Console# show users accounts

Username Privilege

--------- ---------

Bob 15

Robert 15
```

Back to Contents Page

Back to Contents Page

Address Table Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- bridge address
- bridge aging-time
- clear bridge
- show bridge address-table
- show bridge address-table static
- port security
- show ports security
- bridge multicast filtering
- bridge multicast address
- bridge multicast forbidden address
- bridge multicast forward-all
- bridge multicast forbidden forward-all
- show bridge multicast address-table
- show bridge multicast filtering

---

bridge address

Use the **bridge address** interface configuration command to add a static MAC-layer station source address to the bridge table. To delete the MAC address, use the **no** form of the **bridge address** command (using the **no** form of the command without specifying a MAC address deletes all static MAC addresses belonging to this VLAN).

Syntax

bridge address *mac-address* {**ethernet** *interface* | **port-channel** *port-channel-number*} [**permanent** | **delete-on-reset** | **delete-on-timeout** | **secure**]

no bridge address [*mac-address*]

- *mac-address*—A MAC address.
- *interface*—An ethernet port.
- *port-channel-number*—A port-channel number.
- **permanent**—The address can only deleted by the **no bridge address** command.
- **delete-on-reset**—The address is deleted after reset.
- **delete-on-timeout**—The address is deleted after age out time has expired.
- **secure**—The address is deleted after the port changes mode to unlock learning (**no port security** command). This parameter is only available when the port is in learning locked mode.

Default Configuration

No static addresses are defined. The default mode for an added address is **permanent**.

Command Mode

Interface Configuration (VLAN) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example adds a permanent static MAC-layer station source address on a port to the bridge table.

```
Console (config-if)# bridge address 168.210.0.10 ethernet 1/e8 permanent
```

---

bridge aging-time

Use the **bridge aging-time** global configuration command to set the address table aging time. To restore the default, use the **no** form of the command.

Syntax

bridge aging-time *seconds*

no bridge aging-time

- *seconds*—Time is number of seconds. (Range: **10-5000000** seconds)

Default Configuration

The default is **300** seconds.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the bridge aging time.

```
Console (config)# bridge aging-time 250
```

---

clear bridge

Use the **clear bridge** privileged EXEC command to remove any learned entries from the forwarding database.

Syntax

clear bridge

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example clears the bridge tables.

```
Console# clear bridge
```

---

show bridge address-table

Use the **show bridge address-table** privileged EXEC command to display dynamically created entries in the bridge-forwarding database.

Syntax

show bridge address-table [**vlan** *vlan*] [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *vlan*—Specific VLAN, such as VLAN 1.
- *interface*—An ethernet port.
- *port-channel-number*—A port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all classes of entries in the bridge-forwarding database.

```
Console# show bridge address table

Aging time is 300 sec

vlan mac address port type

---- -------------- ----- -----

1 0060.704C.73FF 5/8 dynamic

1 0060.708C.73FF 5/8 dynamic

200 0010.0D48.37FF 5/9 static
```

---

show bridge address-table static

Use the **show bridge address-table** privileged EXEC command to display statically entered entries in the bridge-forwarding database.

Syntax

show bridge address-table static [**vlan** *vlan*] [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *vlan*—Specific VLAN, such as VLAN 1.
- *interface*—An ethernet port.
- *port-channel-number*—A port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all classes of entries in the bridge-forwarding database.

```
Console# show bridge address table static

Aging time is 300 sec

vlan mac address port type

---- -------------- ----- -----

200 0010.0D48.37FF 5/9 delete-on-reset
```

---

port security

Use the **port security** interface configuration command to disable new address learning on an interface. To enable new address learning, use the **no** form of the command.

Syntax

port security [**forward** | **discard | discard-shutdown**] [**trap** *seconds*]

no port security

- **forward**—Forwards frames with unlearned source addresses, but does not learn the address.
- **discard**—Discards frames with unlearned source addresses. This is the default if no option is indicated.
- **discard-shutdown**—Discards frames with unlearned source addresses. The port is also shut down.
- **trap** *seconds*—Sends SNMP traps and defines the minimal amount of time in seconds between two consecutive traps (Range: **1-1,000,000**)

Default Configuration

Port security is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example disables the learning of new addresses on a port. All frames with unlearned source addresses are discarded.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# port security discard
```

---

show ports security

Use the **show ports security** privileged EXEC command to display the port-lock status.

Syntax

show ports security [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—An ethernet port.
- *port-channel-number*—A port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all classes of entries in the port-lock status.

```
Console # show ports security


Port Action Trap Frequency Counter

---- ----------------- -------- --------- -------

5/7 Discard Enable 100 88

7/8 Discard, Shutdown Disable


Frequency: Trap Frequency

Counter: Number of violations since last trap
```

---

bridge multicast filtering

Use the **bridge multicast filtering** global configuration command to enable filtering of multicast addresses. To disable filtering of multicast addresses, use the **no** form of the command.

Syntax

bridge multicast filtering

no bridge multicast filtering

Default Configuration

Disabled. All multicast addresses are flooded to all ports of the relevant VLAN.

Command Mode

Global Configuration Mode

User Guidelines

If multicast routers exist on the VLAN and IGMP snooping is not enabled, use the **bridge multicast forward-all** command to forward all multicast packets to the multicast routers.

Example

The following example enables bridge multicast filtering.

```
Console (config)# bridge multicast filtering
```

---

bridge multicast address

Use the **bridge multicast address** interface configuration command to register MAC-layer multicast addresses to the bridge table, and adds static ports to the group. To unregister the MAC address, use the **no** form of the **bridge multicast address** command.

Syntax

bridge multicast address {*mac-multicast-address* | *ip-multicast-address*}

bridge multicast address {*mac-multicast-address* | *ip-multicast-address*} {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-number-list* }

no bridge multicast address {*mac-multicast-address* | *ip-multicast-address*}

- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- *mac-multicast-address*—MAC multicast address.
- *ip-multicast-address*—IP multicast address.
- *interface-list*—Separates non-consecutive ethernet ports with a comma and no spaces. A hyphen is used to designate a range of ports.
- *port-channel-number-list*—Separates non-consecutive port-channels with a comma and no spaces. A hyphen is used to designate a range of ports.

Default Configuration

No multicast addresses are defined.

Command Mode

Interface Configuration (VLAN) Mode

User Guidelines

If the command is executed without **add** or **remove**, the command only registers the group in the bridge database.

Static multicast addresses can only be defined on static VLANs.

Examples

The following example registers the MAC address.

```
Console (config)# interface vlan 8

Console (config-if)# bridge multicast address 0100.5e02.0203
```

The following example registers the MAC address and adds ports statically.

```
Console (config)# interface vlan 8

Console (config-if)# bridge multicast address 0100.5e02.0203 add ethernet 1/e1-9, 2/e2
```

---

bridge multicast forbidden address

Use the **bridge multicast forbidden address** interface configuration command to prevent adding a specific multicast address to specific ports. To reconfigure the default value, use the **no** form of this command.

Syntax

bridge multicast forbidden address {*mac-multicast-address* | *ip-multicast-address*} {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-number-list* }

no bridge multicast forbidden address {*mac-multicast-address* | *ip-multicast-address*}

- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- *mac-multicast-address*—MAC multicast address.
- *ip-multicast-address*—IP multicast address.
- *interface-list*—Separate non-consecutive ethernet ports with a comma and no spaces; hyphen is used to designate a range of ports.
- *port-channel-number-list*—Separate non-consecutive port-channels with a comma and no spaces. A hyphen is used to designate a range of port-channels.

Default Configuration

No forbidden addresses are defined.

Command Modes

Interface Configuration (VLAN) Mode

User Guidelines

Register the multicast group before you define the forbidden ports.

Example

The following example forbids the MAC address on port 2/e9 within VLAN 8.

```
Console (config)# interface vlan 8

Console (config-if)# bridge multicast address 0100.5e02.0203

Console (config-if)# bridge multicast forbidden 0100.5e02.0203 add ethernet 2/e9
```

---

bridge multicast forward-all

Use the **bridge multicast forward-all** interface configuration command to forbid a port to be a Forward-all-multicast port. To restore the default, use the **no** form of the **bridge multicast forward-all** command.

Syntax

bridge multicast forward-all {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}

no bridge multicast forward-all

- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- *interface-list*—Separates non-consecutive valid ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list*—Separates non-consecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

Disables forward-all on all ports

Command Mode

Interface Configuration (VLAN) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example forwards all multicast packets on port 1/e8.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# bridge multicast forward-all add ethernet 1/e8
```

---

bridge multicast forbidden forward-all

Use the **bridge multicast forbidden forward-all** interface configuration command to forbid a port to be a Forward-all-multicast port. To restore the default, use the **no** form of this command.

Syntax

bridge multicast forbidden forward-all {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}

no bridge multicast forward-all

- **add**—Forbids forwarding all multicast packets.
- **remove**—Do not forbid forwarding all multicast packets.
- *interface-list*—Separate non-consecutive valid ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list*—Separate non-consecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

By default, this setting is disabled (for example, forwarding to the port is not forbidden).

Command Mode

Interface Configuration (VLAN) Mode

User Guidelines

IGMP snooping dynamically discovers multicast router ports. When a multicast router port is discovered, all the multicast packets are forwarded to it unconditionally. This command prevents a port to be a multicast router port .

Example

The following example forbids forwarding all multicast packets to port 1/e6.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# bridge multicast forbidden forward-all add ethernet 1/e6
```

---

show bridge multicast address-table

Use the **show bridge multicast address-table** privileged EXEC command to display multicast MAC address table information.

Syntax

show bridge multicast address-table [**vlan** *vlan-id*] [**address** *mac-multicast-address* | *ip-multicast-address*] [**format** ip | mac]

- *vlan_id*—A VLAN ID value.
- *mac-multicast-address*—A MAC multicast address.
- *ip-multicast-address*—An IP multicast address.
- **format**—Multicast address format. Can be **ip** or **mac**.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays multicast MAC address table information.

```
Console # show bridge multicast address-table format mac



Vlan MAC Address type Ports

---- -------------- ----- -------------------

1 0100.5e02.0203 static 1/e1, 2/e2

19 0100.5e02.0208 static 1/e1-8

19 0100.5e02.0208 dynamic 1/e9-11



Forbidden ports for multicast addresses:

Vlan MAC Address Ports

---- -------------- -------------------

1 0100.5e02.0203 2/e8

19 0100.5e02.0208 2/e8
```

---

show bridge multicast filtering

Use the **show bridge multicast filtering** privileged EXEC command to display the multicast filtering configuration.

Syntax

show bridge multicast filtering *vlan-id*

- *vlan_id*—A VLAN ID value.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example illustrates the multicast configuration.

```
Console # show bridge multicast filtering 1

Filtering: Enabled

VLAN: 1

Port Forward-All

Static Status

------ --------- ------

1/e1 Forbidden Filter

1/e2 Forward Forward(s)

1/e3 - Forward(s)
```

Back to Contents Page

Back to Contents Page

Command Groups

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

The Command Line Interface (CLI) is a network management application operated through an ASCII terminal without the use of a Graphic User Interface (GUI) driven software application. By directly entering commands, the user has greater configuration flexibility. The CLI is a basic command-line interpreter similar to the UNIX C shell.

A device can be configured and maintained by entering commands from the CLI, which is based solely on textual input, and output with commands being entered by a terminal keyboard and the output displayed as text via a terminal monitor. The CLI can be accessed from a console terminal connected to an EIA/TIA-232 port or through a Telnet session.

This guide describes the Command Line Interface (CLI) structure, the command syntax, and command functionality. The following table contains the functional groups for commands.

Command Group	**Description**
AAA	Configures connection security including authorization and passwords.
Address Table	Configures bridging address tables.
Configuration and Image Files	Manages the device configuration files.
Ethernet Configuration	Configures all port configuration options, for example ports, storm control, port speed and auto-negotiation.
GVRP	Configures and displays GVRP configuration and information.
IGMP Snooping	Configures IGMP snooping and displays IGMP configuration and IGMP information.
IP Addressing	Configures and manages IP addresses on the device.
LACP	Configures and displays LACP information.
Line	Configures the console and remote Telnet.
Management ACL	Configures and displays management access-list information.
Port Channel	Configures and displays port-channeling information.
Port Monitor	Monitors activity on specific target ports.
QoS and ACL	Configures and displays ACL and QoS information.
Radius	Configures and displays the Radius information.
RMON	Displays RMON statistics.

SNMP	Configures SNMP communities, traps and displays SNMP information.
Spanning Tree	Configures and reports on the Spanning Tree protocol.
SSH	Configures SSH authentication.
Syslog Commands	Manages and displays syslog messages.
System Management	Configures the device clock, name and authorized users.
User Interface	Describes user commands used for entering CLI commands.
VLAN	Configures VLANS and displays VLAN information.
Web Server	Configures access to the device.

Command Groups

NOTE: The access mode shown in the following tables is indicated by these abbreviations: UE (User EXEC Mode), PE (Privileged EXEC Mode), GC (Global Configuration Mode), IC (Interface Configuration Mode), LC (Line Configuration) MA (Management Access-level), KC (Key Chain), and VC (VLAN Configuration).

AAA Commands

Command	Description	Mode
aaa authentication login	Defines login authentication.	GC
aaa authentication enable	Defines authentication method lists for accessing higher privilege levels.	GC
login authentication	Specifies the login authentication method list for a remote Telnet or console.	GC
enable authentication	Specifies the authentication method list when accessing a higher privilege level from a remote Telnet or console.	LC
ip http authentication	Specifies authentication methods for http.	GC
ip https authentication	Specifies authentication methods for https.	GC
show authentication methods	Displays information about the authentication methods.	PE
password	Specifies a password on a line.	LC
enable password	Sets a local password to control access to normal and privilege levels.	GC
username	Establishes a user name-based authentication system.	GC
show users accounts	Displays information about the local user database.	PE

Address Table Commands

Command	Description	Mode

bridge address	Adds a static MAC-layer station source address to the bridge table.	VC
bridge aging-time	Sets the address table aging time.	GC
clear bridge	Removes any learned entries from the forwarding database.	PE
show bridge address-table	Displays dynamically created entries in the bridge-forwarding database.	PE
show bridge address-table static	Displays statically entered entries in the bridge-forwarding database.	PE
port security	Disables new address learning on an interface.	IC
show ports security	Displays the port-lock status.	PE
bridge multicast filtering	Enables filtering of multicast addresses.	GC
bridge multicast address	Registers MAC-layer multicast addresses to the bridge table, and adds static ports to the group.	IC
bridge multicast forbidden address	Forbids adding a specific multicast address to specific ports.	IC
bridge multicast forward-all	Enables forwarding of all multicast packets on a port.	IC
bridge multicast forbidden forward-all	Forbids forwarding of all multicast packets to a port.	IC
show bridge multicast address-table	Displays multicast MAC address table information.	PE
show bridge multicast filtering	Displays the multicast filtering configuration.	PE

Configuration and Image Files Commands

Command	Description	Mode
configure	Enters global configuration mode.	PE
copy	Copies any file from a source to a destination.	PE
delete startup-config	Deletes the startup-config file.	PE
boot system	Specifies the system image that the device loads at startup.	GC
show running-config	Displays the contents of the currently running configuration file.	PE
show startup-config	Displays the startup configuration file contents.	PE
show backup-config	Displays the backup configuration file contents.	PE
show bootvar	Displays the active system image file that the device loads at startup.	PE

Ethernet Configuration Commands

Command	Description	Mode
port storm-control enable	Enables broadcast storm control.	IC
port storm-control rate	Configures the maximum broadcast rate.	IC
interface ethernet	Enters the Interface Configuration Mode to configure an ethernet type interface.	GC
interface range ethernet	Enters the Interface Configuration Mode to configure multiple ethernet type interfaces.	GC
shutdown	Disables interfaces.	IC
description	Adds a description to an Interface.	IC
speed	Configures the speed of a given ethernet interface when not using auto negotiation.	IC
duplex	Configures the full/half duplex operation of a given ethernet interface when not using auto negotiation.	IC
negotiation	Enables auto negotiation operation for the speed and duplex parameters of a given interface.	IC
flowcontrol	Configures the flow control on a given interface.	IC
mdix	Enables automatic cable crossover on a given interface.	IC
back-pressure	Enables back pressure on a given interface.	IC
clear counters	Clears statistics on an interface.	PE
set interface active	Reactivates an interface suspended by the system.	PE
show interfaces configuration	Displays the configuration for all configured interfaces.	PE
show interfaces status	Displays the status for all configured interfaces.	PE
show interfaces description	Displays the description for all configured interfaces.	PE
show interfaces counters	Displays traffic seen by the physical interface.	PE
show ports storm-control	Displays the storm control configuration.	PE

GVRP Commands

Command	Description	Mode
gvrp enable (global)	Enables GVRP globally.	GC
gvrp enable (interface)	Enables GVRP on an interface.	IC

garp timer	Adjusts the GARP application join, leave, and leaveall GARP timer values.	IC
gvrp vlan-creation-forbid	Disables dynamic VLAN creation.	IC
gvrp registration-forbid	De-registers all VLANs, and prevents dynamic VLAN registration on the port.	IC
clear gvrp statistics	Clears all the GVRP statistics information.	GC
show gvrp configuration	Displays GVRP configuration information.	PE
show gvrp statistics	Displays GVRP statistics.	PE
show gvrp error-statistics	Displays GVRP error statistics.	PE

IGMP Snooping Commands

Command	Description	Mode
ip igmp snooping (Global)	Enables Internet Group Management Protocol (IGMP) snooping.	GC
ip igmp snooping (Interface)	Enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN.	VC
ip igmp snooping mrouter	Enables automatic learning of multicast device ports in the context of a specific VLAN.	VC
ip igmp snooping host-time-out	Configures the host-time-out.	VC
ip igmp snooping mrouter-time-out	Configures the mrouter-time-out.	VC
ip igmp snooping leave-time-out	Configures the leave-time-out.	VC
show ip igmp snooping mrouter	Displays information on dynamically learned multicast router interfaces.	PE
show ip igmp snooping interface	Displays IGMP snooping configuration.	PE
show ip igmp snooping groups	Displays multicast groups learned by IGMP snooping.	PE

IP Addressing

Command	Description	Mode
ip address	Sets an IP address on the device.	IC
ip address-dhcp	Acquires an IP address on an interface from the DHCP server.	IC
ip default-gateway	Defines default gateways.	IC
show ip interface	Displays a list of IP interfaces configured on the device.	PE
arp	Adds a static entry in the ARP cache.	GC

arp timeout	Configures how long an entry remains in the ARP cache	GC
clear arp-cache	Deletes all dynamic entries from the ARP cache.	PE
show arp	Displays entries in the ARP table.	PE

LACP Commands

Command	Description	Mode
lacp system-priority	Configures the system LACP priority.	GC
lacp port-priority	Configures the priority value for physical ports.	IC
lacp timeout	Assigns an administrative LACP timeout.	IC
show lacp ethernet	Displays LACP information for ethernet ports.	PE
show lacp port-channel	Displays LACP information for a port-channel.	PE

Line Commands

Command	Description	Mode
line	Identifies a specific line for configuration and enters the line configuration command mode.	LC
speed	Sets the line baud rate.	LC
exec-timeout	Configures the interval that the system waits until user input is detected.	LC
show line	Displays line parameters.	UE

Management ACL Commands

Command	Description	Mode
management access-list	Defines an access-list for management, and enters the access-list for configuration.	GC
permit (management)	Defines a permit rule.	MA
deny (management)	Defines a deny rule.	MA
management access-class	Defines which management access-list is used.	GC
show management access-list	Displays the management access-list.	UE
show management access-class	Displays the active management access-list.	UE

Port Channel Commands

Command	Description	Mode
interface port-channel	Enters the interface configuration mode for a specific port-channel.	GC
interface range port-channel	Enters the interface configuration mode to configure multiple port channels.	GC
channel-group	Associates a port with a port-channel.	IC
show interfaces port-channel	Displays port-channel information.	PE

Port Monitor Commands

Command	Description	Mode
port monitor	Starts a port monitoring session.	IC
show ports monitor	Displays the port monitoring status.	UE

QoS and ACL Commands

Command	Description	Mode
ip access-list	Creates IP ACLs and enters IP-Access list configuration mode.	GC
permit (IP)	Allows traffic if the conditions defined in the permit statement are matched.	IP
deny (IP)	Denies traffic if the conditions defined in the deny statement are matched	IP
mac access-list	Creates Layer 2 MAC ACLs, and enters to MAC-Access list configuration mode.	GC
permit (MAC)	Allows traffic if the conditions defined in the permit statement are matched.	ML
deny (MAC)	Allows traffic if the conditions defined in the permit statement are matched.	ML
service-acl	Applies an access-list to the input of an interface.	IC
show access-lists	Displays access control lists (ACLs) defined on the device	PE
show interfaces access-lists	Displays access lists applied on interfaces.	PE
qos	Enables quality of service (QoS) on the device.	GC
show qos	Displays the QoS activity status.	GC
wrr-queue cos-map	Maps assigned CoS values to the egress queues.	GC

wrr-queue bandwidth	Assigns Weighted Round Robin (WRR) weights to egress queues.	IC
priority-queue out num-of-queues	Enables the egress queues to be expedite queues.	IC
show qos interface	Displays interface QoS data.	UE
qos map dscp-queue	Modifies the DSCP to CoS map.	GC
qos trust(Global)	Configures the system trust state.	GC
qos trust(Interface)	Enables each port trust state.	IC
qos cos	Configures the default port CoS value.	IC
qos map tcp-port-queue	Modifies the TCP-Port to DSCP table.	GC
qos map udp-port-queue	Modifies the UDP-Port to DSCP table.	GC
show qos map	Displays all the QoS maps.	UE

Radius Commands

Command	Description	Mode
radius-server host	Specifies a RADIUS server host.	GC
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.	GC
radius-server retransmit	Specifies the number of times the software searches the list of RADIUS server hosts.	GC
radius-server source-ip	Specifies the source IP address used for communication with RADIUS servers.	GC
radius-server timeout	Sets the interval for which a device waits for a server host to reply.	GC
radius-server deadtime	Improves RADIUS response times when servers are unavailable.	GC
show radius-servers	Displays the RADIUS server settings.	UE

RMON Commands

Command	Description	Mode
show rmon statistics	Displays RMON ethernet statistics.	PE
rmon collection history	Enables a Remote Monitoring (RMON) MIB history statistics group on an interface.	IC
show rmon collection history	Displays the requested history group configuration.	PE
show rmon history	Displays RMON ethernet statistics history.	PE

rmon alarm	Configures alarm conditions.	GC
show rmon alarm-table	Displays the alarms summary table.	PE
show rmon alarm	Displays alarm configurations.	PE
rmon event	Configures a RMON event.	GC
show rmon events	Displays the RMON event table.	PE
show rmon log	Displays the RMON logging table.	PE
rmon table-size	Configures the maximum RMON tables sizes.	GC

SNMP Commands

Command	Description	Mode
snmp-server community	Sets up the community access string to permit access to SNMP protocol.	GC
snmp-server contact	Sets up a system contact.	GC
snmp-server location	Enters information on where the device is located.	GC
snmp-server enable traps	Enables the switch to send SNMP traps or SNMP notifications.	GC
snmp-server trap authentication	Enables the switch to send SNMP traps when authentication failed.	GC
snmp-server host	Specifies the recipient of SNMP notification operation.	GC
snmp-server set	Sets SNMP MIB value by the CLI.	GC
show snmp	Displays the SNMP status.	PE

Spanning Tree Commands

Command	Description	Mode
spanning-tree	Enables spanning tree functionality.	GC
spanning-tree mode	Configures the spanning tree protocol currently running.	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 priority.	GC
spanning-tree disable	Disables spanning tree on a specific port.	IC
spanning-tree cost	Configure the spanning tree path cost for a port.	IC
spanning-tree port-priority	Configures the port priority.	IC
spanning-tree portfast	Enable PortFast mode.	IC
clear spanning-tree detected-protocols	Restarts the protocol migration process on all interfaces or on the specified interface.	PE
spanning-tree link-type	Overrides the default link-type setting.	IC
show spanning-tree	Displays spanning tree configuration.	PE

SSH Commands

Command	Description	Mode
ip ssh port	Specifies the port for use by the SSH server.	GC
ip ssh server	Enables device configuration from a SSH server.	GC
crypto key generate dsa	Generates DSA key pairs.	GC
crypto key generate rsa	Generates RSA key pairs.	GC
ip ssh pubkey-auth	Enables public key authentication for incoming SSH sessions.	GC
crypto key pubkey-chain ssh	Enters SSH public key-chain configuration mode.	GC
user-key	Specifies which SSH public key is manually configured and enters the SSH public key-string configuration command.	KC
key-string	Manually specifies a SSH public key.	KC
show ip ssh	Displays the SSH server configuration.	PE
show crypto key mypubkey	Manually specifies a SSH public key.	PE
show crypto key pubkey-chain ssh	Displays SSH public keys stored on the device.	PE

Syslog Commands

Command	Description	Mode
logging on	Controls error messages logging.	GC

logging	Logs messages to a syslog server.	GC
logging console	Limits messages logged to the console based on severity.	GC
logging buffered	Limits syslog messages displayed from an internal buffer based on severity.	GC
logging buffered size	Changes the number of syslog messages stored in the internal buffer.	GC
clear logging	Clears messages from the internal logging buffer.	PE
logging file	Limits syslog messages sent to the logging file based on severity.	GC
clear logging file	Clears messages from the logging file.	PE
show logging	Displays the state of logging and the syslog messages stored in the internal buffer.	PE
show logging file	Displays the state of logging and the syslog messages stored in the logging file.	PE
show syslog-servers	Displays the syslog servers settings.	PE

System Management Commands

Command	Description	Mode
ping	Sends ICMP echo request packets to another node on the network.	UE
reload	Reloads the operating system.	PE
clock set	Manually sets the system clock.	UE
hostname	Specifies or modifies the device host name.	GC
asset-tag	Specifies the device asset-tag.	GC
stack order	configures the unit physical order in the stack.	GC
show users	Displays information about the active users.	UE
show clock	Displays the time and date from the system clock.	UE
show system	Displays system information.	UE
show version	Displays the system version information.	PE
show system id	Displays the system identification information.	PE

User Interface Commands

Command	Description	Mode

enable	Enters the privileged EXEC mode.	UE
disable	Returns the prompt to user EXEC mode.	PE
login	Exits the EXEC mode and re-logs on as a new user.	PE
exit(configuration)	Exits any configuration mode to the next highest mode in the CLI mode hierarchy.	
exit(EXEC)	Closes an active terminal session by logging off the device.	UE
end	Ends the current configuration session and returns to the previous command mode.	GC
help	Displays a brief description of the help system.	
history	Enables the command history function.	LC
history size	Changes the command history buffer size for a particular line.	LC
debug-mode	Switches the mode to debug the device.	PE
show history	Lists the commands entered in the current session.	PE
show privilege	Displays the current privilege level.	PE

VLAN Commands

Command	Description	Mode
vlan database	Enters the VLAN database configuration mode.	GC
vlan	Creates a VLAN.	VC
interface vlan	Enters the interface configuration (VLAN) mode to configure an existing VLAN.	GC
interface range vlan	Enters the VLAN configuration mode to configure multiple VLANs.	GC
name	Configures a name to a VLAN.	VC
switchport mode	Configures the VLAN membership mode for a port.	IC
switchport access vlan	Configures the VLAN ID when the interface is in access mode.	IC
switchport trunk allowed vlan	Adds or removes VLANs from a trunk port.	IC
switchport trunk native vlan	Defines the port as a member of the specified VLAN, and the VLAN ID is the port default VLAN ID (PVID).	IC
switchport general allowed vlan	Adds or removes VLANs from a port in general mode.	IC

switchport general pvid	Configures the PVID when the interface is in general mode.	IC
switchport general ingress-filtering disable	Disables port ingress filtering	IC
switchport general acceptable-frame-types tagged-only	Discards untagged frames at ingress.	IC
switchport forbidden vlan	Forbids adding specific VLANs to a port.	IC
show vlan	Displays VLAN information.	PE
show interfaces switchport	Displays switchport configuration.	PE

Web Server Commands

Command	Description	Mode
ip http port	Specifies the TCP port for use by a web browser to configure the device.	GC
ip http server	Enables the device to be configured from a browser.	GC
ip https port	Configures a TCP port for use by a secure web browser to configure the device.	GC
ip https server	Enables the device to be configured from a secured browser.	GC
crypto certificate generate	Generates a HTTPS certificate.	GC
show ip http	Displays the HTTP server configuration.	PE
show ip https	Displays the HTTPS server configuration.	PE

Back to Contents Page

Back to Contents Page

Configuration and Image Files

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- configure
- copy
- delete startup-config
- boot system
- show running-config
- show startup-config
- show backup-config
- show bootvar

---

configure

The **configure** privileged EXEC command enters global configuration mode.

Syntax

configure

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

In the following example, a prompt is displayed because no keyword is entered. After the keyword is selected, a message confirming the command entry method is displayed.

```
Console # configure


Console(config)#
```

---

copy

Use the **copy** privileged EXEC command to copy files from a source to a destination.

Syntax

copy *source-url destination-url*

- *source-url*—The source file location URL or reserved keyword being copied.
- *destination-url*—The destination file URL or reserved keyword.

The following table describes keywords for sources or destinations:

Keyword	Source or destination
running-config	Copy from the current running configuration file.-- Only to another configuration file, or to a TFTP server
startup-config	Copy from the startup configuration file.-- Only to the backup-config file or to a TFTP server
backup-config	Copy from the backup configuration file. -- Only to the startup-config file or a TFTP server
image	If the source represents the active image file, destination represents the inactive image file.
boot	Copy from the BOOT file -- Only to a TFTP server or another unit (if stacked).
tftp:	Source URL (tftp://ip address/filename) for a file on a TFTP network server from which to download. The syntax for this alias is **tftp:**[[//location]/directory]/filename.
xmodem:	Source for the file from a serial connection that uses the Xmodem protocol.
unit://member/startup-config	Configuration file used during initialization (startup) on one of the units. To copy a file to all the units use all as device name.
unit://member/backup-config	Backup configuration file on one of the units. To copy a file to all the units use all as device name.
unit://member/image	Image file on one of the units. To copy a file to all the units use all as device name.
unit://member/boot	Boot file on one of the units. To copy a file to all the units use all as device name.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

The location of a file system dictates the format of the source or destination URL.

The startup-config and the backup-config files cannot be copied to the running-config file.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

Understanding Invalid Combinations of Source and Destination

Some invalid combinations of source and destination files exist. Specifically, the following cannot be copied:

- If the source file and destination file are the same file.

- **boot** and **image** cannot be a source file.
- **xmodem** cannot be a destination.
- **tftp** cannot be the source and destination on the same copy.

The following table describes characters used in the copy process.

Character	Description
!	For network transfers, an exclamation point indicates that the copy process is taking place. Each exclamation point indicates the successful transfer of ten packets (512 bytes each).
.	For network transfers, a period indicates that the copy process timed out. Many periods in a row typically mean that the copy process may fail.

Copying a system image file from a Server to Flash Memory

Use the copy source-url image command to copy a system image file from a server to Flash memory.

Copying boot file from a Server to Flash Memory

Use the **copy source-url boot** command to copy a boot file from a server to Flash memory.

Copying a Configuration File from a Server to the Running Configuration

Use the **copy source-url running-config** command to load a configuration file from a network server to the device running configuration. The configuration is added to the running configuration as if the commands were typed in the command-line interface (CLI). The resulting configuration file is a combination of the previous running configuration and the loaded configuration file, with the loaded configuration file having precedence.

Copying a Configuration File from a Server to the Startup Configuration

Use the **copy source-url startup-config** command to copy a configuration file from a network server to the device startup configuration. These commands replace the startup configuration file with the copied configuration file.

Storing the Running or Startup Configuration on a Server

Use the copy **running-config destination-url** command to copy the current configuration file to a network server using TFTP. Use the copy **startup-config destination-url** command to copy the startup configuration file to a network server.

The configuration file copy can serve as a backup copy.

Saving the Running Configuration to the Startup Configuration

Use the copy **running-config startup-config** command to copy the running configuration to the startup configuration file.

Backup the Running Configuration or Startup Configuration to the Backup Configuration

Use the copy **running-config backup-config** command to backup the running configuration to the backup configuration file. Use the copy **startup-config backup-config** command to backup the startup configuration to the backup configuration file.

Example

The following example copies a system image from the TFTP server with an IP address of 172.16.101.101 to a non-active image file.

```
Console # copy tftp://172.16.101.101/file1 image

Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

---

delete startup-config

Use the **delete startup-config** privileged EXEC command to delete the **startup-config** file.

Syntax

delete startup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example deletes the **startup-config** file.

```
Console# delete startup-config

Startup file was deleted.

Console#
```

---

boot system

Use the **boot system** global configuration command to specify the system image that the device loads at startup.

Syntax

boot system [**unit** *unit*] {**image-1** | **image-2**}

- **image-1**—Specifies image 1 as the system startup image.
- **image-2**—Specifies image 2 as the system startup image.
- **unit** *unit*—Unit number. If unspecified, the default is the master unit number.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

Use the **show bootvar** command to find out which image is the active image.

Examples

The following example loads **system image 1** for the next device startup.

```
Console# boot system image-1
```

---

show running-config

Use the **show running-config** privileged EXEC command to display the contents of the currently running configuration file contents.

Syntax

show running-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the **running-config** file contents.

```
Console# show running-config

Building configuration...


Current configuration:

!

version 12.1

!

.
```

```
.

.

interface FastEthernet1/e1

ip address 176.242.100.100 255.

ip pim dense-mode

duplex auto

speed auto

!

.

.

.

end
```

---

show startup-config

Use the **show startup-config** privileged EXEC command to display the startup configuration file contents.

Syntax

show startup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the **startup-config** file contents.

```
Console# show startup-config

Using 1132 out of 29688 bytes

!

version 12.1

!

.

.

.

interface FastEthernet1/e1

ip address 176.242.100.100 255.

ip pim dense-mode

duplex auto

speed auto

!

.

.

.
```

```
end
```

---

show backup-config

Use the show backup-config privileged EXEC command to display the backup configuration file contents.

Syntax

show backup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the contents of the **backup-config** file.

```
Console# show backup-config

Using 1132 out of 29688 bytes

!

version 12.1

!

.

.
```

```
.

interface FastEthernet1/e1

ip address 176.242.100.100 255.

ip pim dense-mode

duplex auto

speed auto

!

.

.

.

end
```

---

show bootvar

Use the show bootvar privileged EXEC command to display the active system image file that the device loads at startup.

Syntax

show bootvar

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the active system image file that the device loads at startup

```
Console# show bootvar

Images currently available on the FLASH

image-1 active (selected for next boot)

image-2 not active
```

Back to Contents Page

Back to Contents Page

Ethernet Configuration Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- port storm-control enable
- port storm-control rate
- interface ethernet
- interface range ethernet
- shutdown
- description
- speed
- duplex
- negotiation
- flowcontrol
- mdix
- back-pressure
- clear counters
- set interface active
- show interfaces configuration
- show interfaces status
- show interfaces description
- show interfaces counters
- show ports storm-control

---

port storm-control enable

Use the **port storm-control enable** global configuration command to enable broadcast storm control. To disable broadcast storm control, use the **no** form of this command.

Syntax

port storm-control enable {**unknown** | **broadcast** | **multicast**} {**fastethernet** | **gigaethernet** *interface*}

no port storm-control enable {**unknown** | **broadcast** | **multicast**} {**fastethernet** | **gigaethernet** *interface*}

- **unknown**—Enables storm control for packets with destination address not found in the MAC forwarding table.
- **broadcast**—Enables storm control for broadcast packets.
- **multicast**—Enables storm control for multicast packets.
- **fastethernet**—Enables storm control for FastEthernet ports.
- **gigaethernet** *interface*—GigaEthernet port number.

Default Configuration

Broadcast storm control is disabled.

Command Modes

Global Configuration Mode

User Guidelines

Use the port **storm-control broadcast rate fastethernet gigaethernet** interface configuration command to set the maximum rate.

Example

The following example enables broadcast storm control for fast ethernet.

```
Console(config)# port storm-control enable broadcast fastethernet
```

---

port storm-control rate

Use the **port storm-control rate** global configuration command to configure the maximum broadcast rate. To reconfigure the default broadcast rate, use the **no** form of this command.

Syntax

port storm-control rate gigaethernet *interface rate*

port storm-control rate fastethernet *rate*

no port storm-control rate gigaethernet *interface*

no port storm-control rate fastethernet

- **gigaethernet** *interface*—GigaEthernet port number
- *rate*—Maximum number of packets per second (Range: **FE: 250 -148000**, **GE: 250-262143**).

Default Configuration

The default frames per second are as follows:

- **FastEthernet—148000**
- **GigaEthernet—262143**

Command Mode

Global Configuration Mode

User Guidelines

Use the **port storm-control broadcast enable** interface configuration command to enable broadcast storm control.

Example

The following example configures the maximum broadcast storm control fast ethernet frame rate.

```
```

```
Console(config)# port storm-control rate fastethernet 300
```

---

interface ethernet

Use the **interface ethernet** global configuration command to enter the interface configuration mode to configure an ethernet type interface.

Syntax

interface ethernet *interface*

- *interface*—An ethernet port. The full syntax is: *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables ports 1/e18 for configuration.

```
Console (config)# interface ethernet 1/e18

Console (config-if)#
```

---

interface range ethernet

Use the **interface range ethernet** global configuration command to enter the interface configuration mode and configure multiple ethernet type interface.

Syntax

interface range ethernet { *port-range* | **all** }

- *port-range*—List of ports to add. Separate non-consecutive ports with a comma and no spaces. A hyphen is used to designate a range of ports.
- **all**—All ethernet ports.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

The interface range ethernet commands are executed independently on each interface in the range. If the command returns an error on one of the interfaces, it does not stop executing on other interfaces.

Example

The following example groups ports to receive the same command.

```
Console (config)# interface range ethernet 1/e18-20, 3/e1-24

Console (config-if)#
```

---

shutdown

Use the **shutdown** interface configuration command to disable the interfaces. To restart a disabled interface, use the **no** form of this command.

Syntax

shutdown

no shutdown

Default Configuration

The interface is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example disables ethernet port 1/e5.

```
Console (config)# interface ethernet 1/e5

Console (config-if)# shutdown
```

The following example re-enables ethernet port 1/e5.

```
Console (config)# interface ethernet 1/e5

Console (config-if)# no shutdown
```

---

description

Use the **description** interface configuration command to add a description to an interface. To remove the description use the **no** form of this command.

Syntax

description *string*

no description

- *string*—Comment or a description of the port, up to 64 characters.

Default Configuration

The interface does not have a description.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example adds the description RD SW#3 to the ethernet port 1/e5.

```
Console (config)# interface ethernet 1/e5

Console (config-if)# description RD SW#3
```

---

speed

Use the **speed** interface configuration command to configure the speed of a given ethernet interface when not using auto negotiation. To restore the default, use the **no** form of this command.

Syntax

speed {**10** | **100** | **1000**}

no speed

- **10**—Configures the port to operate at 10 Mbps.
- **100**—Configures the port to operate at 100 Mbps.
- **1000**—Configures the port to operate at 1000 Mbps.

Default Configuration

Maximum port capability.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

The **no speed** command in port-channel context returns each port in the port-channel to its maximum capability.

Example

The following example configures ethernet port 1/e5 to operate at a speed of 100 Mbps.

```
Console (config)# interface ethernet 1/e5

Console (config-if)# speed 100
```

---

duplex

Use the **duplex** interface configuration command to configure the full/half duplex operation of a given ethernet interface when not using auto negotiation. To restore the default, use the **no** form of this command.

Syntax

duplex {**half** | **full**}

no duplex

- **half**—Forces a half-duplex operation
- **full**—Forces a full-duplex operation

Default Configuration

The interface is set to full duplex.

Command Mode

Interface Configuration (Ethernet) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the duplex operation of ethernet port 1/e5 to operate at full duplex.

```
Console (config)# interface ethernet 1/e5

Console (config-if)# duplex full
```

negotiation

Use the **negotiation** interface configuration command to enable auto negotiation operation for the speed and duplex parameters of a given interface. To disable negotiation, use the **no** form of this command.

Syntax

negotiation

no negotiation

Default Configuration

Auto negotiation is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

Flow control will operate only if duplex mode is set to **FULL**. Back pressure will operate only if duplex mode is set to **HALF**.

When flow control is **ON**, the head-of-line mechanism for this port is disabled.

If a link is set to NOT use auto negotiation, the other side of the link should also be configured to not use auto negotiation, or the link may not operate correctly.

Example

The following example enables autonegotiation on port 1/e5.

```
Console (config)# interface ethernet 1/e5

Console (config-if)# negotiation
```

flowcontrol

Use the **flowcontrol** interface configuration command to configure the flow control on a given interface. To restore the default, use the **no** form of this command.

Syntax

flowcontrol {**auto | on** | **off | rx | tx**}

no flowcontrol

- **auto**—Enables auto negotiation of flow control.
- **on**—Enables flow control.
- **off**—Disables flow control.
- **rx**—Enables only receiving pause frames.
- **tx**—Enables only transmitting pause frames.

Default Configuration

Flow control is off.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode.

User Guidelines

Flow control can be enabled only if duplex mode is set to full-duplex.

Example

The following example enables flow control on port 1/e5.

```
Console (config)# interface ethernet 1/e5

Console (config-if)# flowcontrol on
```

---

mdix

Use the **mdix** interface configuration command to enable automatic crossover on a given interface. To disable automatic crossover, use the **no** form of this command.

Syntax

mdix {**on | auto**}

no mdix - sets port to MDI

- **on**—Manual mdix
- **auto**—Auto mdi/mdix

Default Configuration

Automatic crossover is enabled.

Command Mode

Interface Configuration (Ethernet) Mode

Example

The following example enables automatic crossover on port 1/e5.

```
Console (config)# interface ethernet 1/e5

Console (config-if)# mdix auto
```

.

---

back-pressure

Use the **back-pressure** interface configuration command to enable back pressure on a given interface. To disable back pressure, use the **no** form of this command.

Syntax

back-pressure

no back-pressure

Default Configuration

Back pressure is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example enables back pressure on port 1/e5.

```
Console (config)# interface ethernet 1/e5

Console (config-if)# back-pressure
```

---

clear counters

Use the **clear counters** Privileged EXEC Mode command to clear statistics on an interface.

Syntax

clear counters {**ethernet** *interface* | **port-channel** *port-channel-number*}

- *interface*—An ethernet port. The full syntax is: *unit/port*.
- *port-channel-number*—A port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example clears the counters for interface 1/e1.

```
Console# clear counters ethernet 1/e1
```

---

set interface active

Use the **set interface up** Privileged EXEC Mode command to reactivate an interface suspended by the system.

Syntax

set interface active {**ethernet** *interface* | **port-channel** *port-channel-number*}

- *interface*—An ethernet port. The full syntax is: *unit/port*.
- *port-channel-number*—A port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

This command is used to activate interfaces that were configured to be active, but were shut down for example, for a security violation.

Example

The following example activates interface 1/e5 which is disabled.

```
Console# set interface active ethernet 1/e5
```

---

show interfaces configuration

Use the **show interfaces configuration** privileged EXEC command to display the configuration for all configured interfaces.

Syntax

show interfaces configuration [**ethernet** *interface* | **port-channel** *port-channel-number*]

- **ethernet** *interface*—A ethernet port. The full syntax is: *unit/port*.
- **port-channel** *port-channel-number*—A port-channel index.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration for all configured interfaces.

```
Console# show interfaces configuration


Port Type Duplex Speed Neg Flow Admin Back MDIX
 Cont State Pres Mode
---- ---------- ------ ----- ---- ---- ---- ----- -----
1/e1 1g-combo-c Full 1000 Auto On Up Enable Auto
2/e1 100-copper Full 1000 Off Off Up Disable off


2/e2 1g-Fiber Full 1000 Off Off Up Disable on


Neg : Negotiation
Flow Cont: Flow Control
Back Pres: Back Pressure
```

The displayed port configuration information includes the following:

- **Port**—The port number.
- **Description**—If the port has a description, the description is displayed.
- **Port Type**—The port designated IEEE shorthand identifier. For example, 1000Base-T refers to 1000 Mbps baseband signaling including both Tx and Rx transmissions.
- **Duplex**—Displays the port duplex status.
- **Speed**—Refers to the port speed.
- **Neg**—Describes the auto-negotiation status.
- **Flow Cont**—Displays the flow control status.
- **Back Pres**—Displays the back pressure status.

- **Auto MDIX**—Displays the auto-crossover status.
- **Admin State**—Displays whether the port is enabled or disabled.

---

show interfaces status

Use the **show interfaces status** privileged EXEC command to display the status for all configured interfaces.

Syntax

show interfaces status [**ethernet** *interface* | **port-channel** *port-channel-number*]

- **ethernet** *interface*—An Ethernet port. The full syntax is: *unit/port*.
- **port-channel** *port-channel-number*—A port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the status for all configured interfaces.

```
Console# show interfaces status

 Port Type Duplex Speed Neg Flow Link Back MDI
  Cont State Pres Mode
 ---- ---------- ------ ----- ---- ---- ---- ---- -----
 1/e1 1g-Combo-c Full 100 Auto On Up Enable Off
 2/e1 100-copper Full 1000 off Off Down* Disable Down*

2/e2 1g-Fiber Full 1000 Off Off Up Disable Up
```

```
Legend


Neg : Negotiation


Flow Cont: Flow Control


Back Pres: Back Pressure


*: The interface was suspended by the system.
```

The displayed port status information includes the following:

- **Port**—The port number.
- **Port Type**—The port designated IEEE shorthand identifier. For example, 1000Base-T refers to 1000 Mbps baseband signaling including both Tx and Rx transmissions.
- **Duplex**—Displays the port duplex status.
- **Speed**—Refers to the port speed.
- **Neg**—Describes the auto-negotiation status.
- **Flow Cont**—Displays the flow control status.
- **Back Pres**—Displays the back pressure status.
- **Link State**—Displays the link aggregation status.

---

show interfaces description

The **show interfaces description** privileged EXEC command displays the description for all configured interfaces.

Syntax

show interfaces description [**ethernet** *interface* | **port-channel** *port-channel-number* | **out-of-band-eth** *oob-interface*]

- **ethernet** *interface*—An Ethernet port. The full syntax is: unit/port.
- **port-channel** *port-channel-number*—A port-channel index.
- **out-of-band-eth** *oob-interface*—Out-of-band interface.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the description for all configured interfaces.

```
device# show interfaces description


Port Description

---- ----------------------------------------------------- ------------

1/e1 Port that should be used for management only

2/e1

2/e2



Port Channel Description

------------ -----------

1 dell

2 projects
```

---

show interfaces counters

The **show interfaces counters** privileged EXEC command displays traffic seen by a physical interface.

Syntax

show interfaces counters [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—An Ethernet port. The full syntax is: *unit/port*.
- *port-channel-number*—A port-channel index.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays traffic seen by the physical interface.

```
Console# show interfaces counters

Port InOctets InUcastPkts InMcastPkts InBcastPkts

---- ---------- --------- --------- ------------

1/e1 183892 1289 987 8

2/e1 0 0 0 0

3/e1 123899 1788 373 19

Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts

---- ---------- --------- --------- ------------

1/e1 9188 9 8 0

2/e1 0 0 0 0

3/e1 8789 27 8 0

Ch InOctets InUcastPkts InMcastPkts InBcastPkts

---- ---------- --------- -------- ------------
```

```
1 27889 928 0 78

Ch OutOctets OutUcastPkts OutMcastPkts OutBcastPkts

---- ---------- --------- --------- ------------

1 23739 882 0 122
```

The following example displays which fields are supported for port 1/e1.

```
Console# show interfaces counters ethernet 1/e1

Port InOctets InUcastPkts InMcastPkts InBcastPkts

---- ---------- --------- --------- ------------

1/e1 183892 1289 987 8

Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts

---- ---------- --------- --------- ------------

1/e1 9188 9 8 0

Alignment Errors: 17

FCS Errors: 8

Single Collision Frames: 0

Multiple Collision Frames: 0

SQE Test Errors: 0

Deferred Transmissions: 0

Late Collisions: 0

Excessive Collisions: 0

Internal MAC Tx Errors: 0
```

```
Carrier Sense Errors: 0

Oversize Packets: 0

Internal MAC Rx Errors: 0

Symbol Errors: 0

Received Pause Frames: 0

Transmitted Pause Frames: 0
```

The following table describes the fields shown in the display:

Field	Description
InOctets	Counts received octets.
InUcastPkts	Counts received unicast packets.
InMcastPkts	Counts received multicast packets.
InBcastPkts	Counts received broadcast packets.
OutOctets	Counts transmitted octets.
OutUcastPkts	Counts transmitted unicast packets.
OutMcastPkts	Counts transmitted multicast packets.
OutBcastPkts	Counts transmitted broadcast packets.
Alignment Errors	Counts frames received that are not an integral number of octets in length and do not pass the FCS check.
FCS Errors	Counts frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames	Counts frames that are involved in a single collision, and are subsequently transmitted successfully.
Multiple Collision Frames	Counts frames that are involved in more than one collision and are subsequently transmitted successfully.
SQE Test Errors	Counts times that the SQE TEST ERROR is received. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 2000 Edition, section 7.2.4.6.
Deferred Transmissions	Counts frames for which the first transmission attempt is delayed because the medium is busy.
Late Collisions	Counts times that a collision is detected later than one slotTime into the transmission of a packet.
Excessive Collisions	Counts frames for which transmission fails due to excessive collisions.
Internal MAC Tx Errors	Counts frames for which transmission fails due to an internal MAC sublayer transmit error.
Carrier Sense Errors	Counts times the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Oversize Packets	Counts frames received that exceed the maximum permitted frame size.
Internal MAC Rx Errors	Counts frames for which reception fails due to an internal MAC sublayer receive error.
Symbol Errors	For an interface operating at 100 Mbps, the number of times there was an invalid data symbol when a valid carrier was present. For an interface operating in half-duplex mode at 1000 Mbps, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate Data reception error or carrier extend error on the GMII. For an interface operating in full-duplex mode at 1000 Mbps, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate Data reception error on the GMII. For an interface operating at 10 Gbps, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate Receive Error on the XGMII.
Received Pause Frames	Counts MAC Control frames received with an opcode indicating the PAUSE operation.
Transmitted Pause Frames	Counts MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.

show ports storm-control

Use the **show ports storm-control** privileged EXEC command to display the storm control configuration.

Syntax

show ports storm-control

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the storm control configuration.

```
Console# show ports storm-control

Port Unknown Broadcast Multicast Rate[Packets/sec]

-------------- -------- --------- -------- -----------------

Gigaethernet 1 Enabled Disabled Enabled 2000

Gigaethernet 2 Enabled Enabled Enabled 2000

FastEthernet Enabled Enabled Enabled 1000
```

Back to Contents Page

Back to Contents Page

GVRP Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- gvrp enable (global)
- gvrp enable (interface)
- garp timer
- gvrp vlan-creation-forbid
- gvrp registration-forbid
- clear gvrp statistics
- show gvrp configuration
- show gvrp statistics
- show gvrp error-statistics

---

gvrp enable (global)

GVRP, or GARP VLAN Registration Protocol, is an industry-standard protocol designed to circulate VLAN information from device to device. With GVRP, a single switch is manually configured with all desired VLANs for the network, and all other switches on the network learn these VLANs dynamically.

The **gvrp enable** global configuration command enables GVRP globally. To disable GVRP globally on the switch, use the **no** form of this command.

Syntax

gvrp enable

no gvrp enable

Default Configuration

GVRP is globally disabled.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example globally enables GVRP on the device.

```
Console (config)# gvrp enable
```

---

gvrp enable (interface)

The **gvrp enable** interface configuration command enables GVRP on an interface. To disable GVRP on an interface, use the **no** form of this command.

Syntax

gvrp enable

no gvrp enable

Default Configuration

GVRP is disabled on all interfaces by default.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

The default port state is **access**, which is a port that belongs to a single, untagged VLAN. GVRP cannot join a port with state as access. To modify the port state, see the command switchport mode.

Example

The following example enables GVRP on port 1/e8.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# gvrp enable
```

---

garp timer

Use the **garp timer** interface configuration command to adjust the GARP application join, leave, and leaveall GARP timer values. To reset the timer to default values, use the **no** form of this command.

Syntax

garp timer {**join** | **leave** | **leaveall**} *timer_value*

no garp timer

- **join**—Indicates the time in milliseconds that PDUs are transmitted.
- **leave**—Indicates the amount of time in milliseconds that the device waits before leaving its GARP state. The leave time is activated by a leave all time message sent/received, and cancelled by the Join message.
- **leaveall**—Used to confirm the port within the VLAN. The time in milliseconds between messages sent.
- *timer_value*—Timer values in milliseconds.

Default Configuration

The default timer values are as follows:

- Join timer—**200** milliseconds
- Leave timer—**600** milliseconds
- Leavall timer—**10000** milliseconds

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

The following relationship must be maintained for the various timer values:

- Leave time must be greater than or equal to three times the join time.
- Leaveall time must be greater than the leave time.

Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on Layer 2-connected devices, GARP applications will not operate successfully.

Example

The following example sets the leave timer for port 1/e8.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# garp timer leave 900
```

---

gvrp vlan-creation-forbid

Use the **gvrp vlan-creation-forbid** interface configuration command to disable dynamic VLAN creation. To enable dynamic VLAN creation, use the **no** form of this command.

Syntax

gvrp vlan-creation-forbid

no gvrp vlan-creation-forbid

Default Configuration

Dynamic VLAN creation is enabled by default.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example disables dynamic VLAN creation on port 1/e8.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# gvrp vlan-creation-forbid
```

---

gvrp registration-forbid

Use the **gvrp registration-forbidden** interface configuration command to de-register all VLANs and prevent dynamic VLAN registration on the port. To allow dynamic registering for VLANs on a port, use the **no** form of this command.

Syntax

gvrp registration-forbid

no gvrp registration-forbid

Default Configuration

Dynamic registering and deregistering for each VLAN on the port is allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how default dynamic registering and deregistering is forbidden for each VLAN on port 1/e8.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# gvrp registration-forbid
```

---

clear gvrp statistics

Use the **clear gvrp statistics** global configuration command to clear all the GVRP statistics information.

Syntax

clear gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—An ethernet interface
- *port-channel-number*—A port-channel index

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example clears all the GVRP statistics information on port 1/e8.

```
Console # clear gvrp statistics ethernet 1/e8
```

---

show gvrp configuration

Use the **show gvrp configuration** privileged EXEC command to display GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.

Syntax

show gvrp configuration [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—An ethernet interface
- *port-channel-number*—A port-channel index

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays GVRP configuration information.

```
Console# show gvrp configuration

GVRP Feature is currently enabled on the switch.

Maximum VLANs: 256, Maximum VLANs after reset: 256.

Port(s) Status Registration Dynamic VLAN Timers (milliseconds)

 Creation Join Leave Leave All

-------- ------- ------------ ------------ ----- ----- ----------

2/1 Enabled Normal Enabled 200 600 10000

4/4 Enabled Normal Enabled 200 600 10000
```

show gvrp statistics

Use the **show gvrp statistics** privileged EXEC command to display GVRP statistics.

Syntax

show gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—An ethernet interface
- *port-channel-number*—A port-channel index

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays GVRP statistics information.

```
Console# show gvrp statistics


GVRP statistics:

---------------

Legend:

rJE : Join Empty Received rJIn : Join In Received

rEmp : Empty Received rLIn : Leave In Received
```

```
rLE : Leave Empty Received rLA : Leave All Received

sJE : Join Empty Sent sJIn : Join In Sent

sEmp : Empty Sent sLIn : Leave In Sent

sLE : Leave Empty Sent sLA : Leave All Sent



Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE sLA

---- --- ---- ---- ---- --- --- --- --- --- ---- --- ---

1/e1 0 0 0 0 0 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0 0 0 0 0 0

1/e4 0 0 0 0 0 0 0 0 0 0 0 0

1/e5 0 0 0 0 0 0 0 0 0 0 0 0

1/e6 0 0 0 0 0 0 0 0 0 0 0 0

1/e7 0 0 0 0 0 0 0 0 0 0 0 0

1/e8 0 0 0 0 0 0 0 0 0 0 0 0
```

---

show gvrp error-statistics

Use the **show gvrp error-statistics** privileged EXEC command to display GVRP error statistics.

Syntax

show gvrp error-statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—An ethernet interface
- *port-channel-number*—A port-channel index

Default Configuration

This command has no default configuration.

Command Mode

Privilege EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays GVRP statistics information.

```
Console# show gvrp error-statistics


GVRP error statistics:

----------------

Legend:

INVPROT : Invalid Protocol Id INVPLEN : Invalid PDU Length

INVATYP : Invalid Attribute Type INVALEN : Invalid Attribute Length

INVAVAL : Invalid Attribute Value INVEVENT : Invalid Event


Port INVPROT INVATYP INVAVAL INVPLEN INVALEN INVEVENT

---- ------- ------- ------- ------ ------- --------

1/e1 0 0 0 0 0 0

1/e2 0 0 0 0 0 0

1/e3 0 0 0 0 0 0
```

```
1/e4 0 0 0 0 0 0

1/e5 0 0 0 0 0 0

1/e6 0 0 0 0 0 0

1/e7 0 0 0 0 0 0

1/e8 0 0 0 0 0 0
```

Back to Contents Page

Back to Contents Page

IGMP Snooping Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- ip igmp snooping (Global)
- ip igmp snooping (Interface)
- ip igmp snooping mrouter
- ip igmp snooping host-time-out
- ip igmp snooping mrouter-time-out
- ip igmp snooping leave-time-out
- show ip igmp snooping mrouter
- show ip igmp snooping interface
- show ip igmp snooping groups

---

ip igmp snooping (Global)

Use the **ip igmp snooping** global configuration command to enable Internet Group Management Protocol (IGMP) snooping. To disable IGMP snooping, use the **no** form of this command.

Syntax

ip igmp snooping

no ip igmp snooping

Default Configuration

IGMP snooping is disabled.

Command Mode

Global Configuration Mode

User Guidelines

None

Example

The following example enables IGMP snooping.

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

---

ip igmp snooping (Interface)

Use the **ip igmp snooping** interface configuration command to enable Internet Group Management Protocol (IGMP) snooping on a specific VLAN. To disable IGMP snooping on a VLAN interface, use the **no** form of this command.

Syntax

ip igmp snooping

no ip igmp snooping

Default Configuration

IGMP snooping is disabled on all VLANs in the set context.

Command Mode

Interface Configuration (VLAN) Mode

User Guidelines

IGMP snooping can only be enabled on static VLANs.

Example

The following example enables IGMP snooping on VLAN 2.

```
Console (config)# interface vlan 2

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

---

ip igmp snooping mrouter

The **ip igmp snooping mrouter** interface configuration command enables automatic learning of multicast router ports in the context of a specific VLAN. To remove automatic learning of multicast router ports, use the **no** form of this command.

Syntax

ip igmp snooping mrouter learn-pim-dvmrp

no ip igmp snooping mrouter learn-pim-dvmrp

Default Configuration

Automatic learning of mrouter ports is enabled.

Command Mode

Interface Configuration (VLAN) Mode

User Guidelines

Auto-learning is performed by either IGMP queries or by listening to PIM (Protocol Independent Multicast) and DVMRP (Distance Vector Multicast Routing Protocol) transmissions, even though these protocols are not participated in/supported on this device (transmission is simply eavesdropped on). The senders are multicast routers, so that ports that have mrouters connected to them may be identified by simply listening.

Multicast router ports can be configured statically by using the bridge multicast forward-all command.

Example

The following example enables automatic learning of multicast router ports on VLANs.

```
Console (config) # interface vlan 2

Console (config-if)# ip igmp snooping mrouter learn-pim-dvmrp
```

---

ip igmp snooping host-time-out

Use the **ip igmp snooping host-time-out** interface configuration command to configure the host-time-out. If an IGMP Report for a multicast group was not received for a host-time-out period, from a specific port, this port is deleted from the member list of that multicast group. To reset to default host-time-out, use the **no** form of this command.

Syntax

ip igmp snooping host-time-out *time-out*

no ip igmp snooping host-time-out

- *time-out*—host timeout in seconds (Range: **1-2147483647**).

Default Configuration

The default host-time-out is **150** seconds.

Command Mode

Interface Configuration (VLAN) Mode

User Guidelines

The timeout should be at least 3 times greater then the query period time of the IGMP device.

Example

The following example configures the host timeout.

```
Console (config)# interface vlan 2

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

---

ip igmp snooping mrouter-time-out

Use the **ip igmp snooping mrouter-time-out** interface configuration command to configure the mrouter-time-out. The mrouter-time-out is used for setting the aging-out time after multicast router ports are automatically learned. To configure the default mrouter-time-out, use the **no** form of this command.

Syntax

ip igmp snooping mrouter-time-out *time-out*

no ip igmp snooping mrouter-time-out

- *time-out*—mrouter timeout in seconds (Range: **1-2147483647**)

Default Configuration

The default value is **300** seconds.

Command Mode

Interface Configuration (VLAN) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the mrouter timeout.

```
Console (config)# interface vlan 2

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

---

ip igmp snooping leave-time-out

Use the **ip igmp snooping leave-time-out** command to configure the leave-time-out. If an IGMP report for a multicast group is not received within the leave-time-out period after an IGMP leave message was received from a specific port, the current port is deleted from the member list of that multicast group. To configure the default leave-time-out, use the **no** form of this command.

Syntax

ip igmp snooping leave-time-out {*time-out* | **immediate-leave**}

no ip igmp snooping leave-time-out

- *time-out*—leave-time-out in seconds (Range: **0-2147483647**).
- **immediate-leave**—Specifies that the port should be immediately removed from the members list after receiving IGMP Leave message.

Default Configuration

The default leave-time-out configuration is **10** seconds.

Command Mode

Interface Configuration (VLAN) Mode

User Guidelines

The leave timeout should be set to greater than the maximum time that a host is allowed to respond to an IGMP Query.

Use **immediate leave** only where there is only one host connected to a port.

The following example configures the host leave-time-out.

```
Console (config)# interface vlan 2
```

```
Console (config-if)# ip igmp snooping leave-time-out 60
```

---

show ip igmp snooping mrouter

Use the **show ip igmp snooping mrouter** privileged EXEC command to display information on dynamically learned multicast router interfaces.

Syntax

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

- *vlan_id*—VLAN ID value.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays IGMP snooping mrouter information on VLAN 1000.

```
Console # show ip igmp snooping mrouter interface 200


VLAN Ports


------- ----------------------------------------


200 1/e1, 2/e1
```

---

show ip igmp snooping interface

Use the **show ip igmp snooping interface** privileged EXEC command to display IGMP snooping configuration.

Syntax

show ip igmp snooping interface *vlan-id*

- *vlan_id*—VLAN ID value.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays IGMP snooping information on VLAN 1000.

```
Console # show ip igmp snooping interface 1000

IGMP Snooping is globally enabled

IGMP Snooping is enabled on VLAN 1000

IGMP host timeout is 300 sec

IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec

IGMP mrouter timeout is 300 sec

Automatic learning of multicast router ports is enabled
```

---

show ip igmp snooping groups

Use the **show ip igmp snooping groups** command to display the multicast groups learned by IGMP snooping.

Syntax

show ip igmp snooping groups [**vlan** *vlan-id*] [**address** *ip-multicast-address*]

- *vlan_id*—VLAN ID value
- *ip-multicast-address*—IP multicast address

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

To see the full multicast address table (including static addresses) use the show bridge address-table command.

Example

The following example displays IGMP snooping information on VLAN 1000.

```
Console # show ip igmp snooping groups

Vlan IP Address Querier Ports

---- ------------------ ------- ------------------

1 224-239.130|2.2.3 Yes 1/1, 2/2

19 224-239.130|2.2.8 Yes 1/9-11
```

Back to Contents Page

Back to Contents Page

IP Addressing Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- ip address
- ip address-dhcp
- ip default-gateway
- show ip interface
- arp
- arp timeout
- clear arp-cache
- show arp

---

ip address

Use the **ip address** interface configuration command to set an IP address. To remove an IP address, use the **no** form of this command.

Syntax

ip address *ip-address* {*mask* | *prefix-length*}

no ip address [*ip-address*]

- *ip-address*—IP address
- *mask*—The IP address network mask
- *prefix-length*—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/) (Range: **0-32**).

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) Mode

User Guidelines

An IP address cannot be configured for a range of interfaces (interface range ethernet command).

Examples

The following example configures VLAN 1 with the IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
Console (config)# interface vlan 1
```

```
Console (config-if)# ip address 131.108.1.27 255.255.255.0
```

---

ip address-dhcp

Use the **ip address-dhcp** interface configuration command to acquire an IP address on an interface from the Dynamic Host Configuration Protocol (DHCP) server. To deconfigure any acquired address, use the **no** form of this command.

The **no ip address-dhcp** command deconfigures any IP address that was acquired, thus sending a DHCPRELEASE message.

Syntax

ip address-dhcp [**hostname** *host-name*]

no ip address-dhcp

- **hostname**—Specifies the host name.
- *host-name*—DHCP host name. This name need not be the same as the host name entered in Global Configuration Mode.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN)

User Guidelines

The **ip address-dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol.

Some DHCP servers require that the DHCPDISCOVER message have a specific host name. The most typical usage of the **ip address-dhcp hostname** *host-name* command is when *host-name* is the host name provided by the system administrator.

If a device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If the **ip address-dhcp** command is used with or without the optional keyword, the DHCP option 12 field (host name option) is included in the DISCOVER message. By default, the specified DHCP host name is the device globally configured host name.

Examples

The following example acquires an IP address on an ethernet interface from DHCP.

```
```

```
Console (config)# interface ethernet 1/e8


Console (config-if)# ip address-dhcp
```

---

ip default-gateway

Use the **ip default-gateway** global configuration command to define default gateways. To remove a default gateway, use the **no** form of this command.

Syntax

ip default-gateway *ip-address1* [*ip-address2*...]

no ip default-gateway [*ip-address*]

- *ip-address*—Default gateway IP address.

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration Mode

User Guidelines

Multiple gateways can be configured, but only one can be active.

Examples

The following example defines a default gateway with the IP address 196.210.10.1.

```
Console (config)# ip default-gateway 196.210.10.1
```

---

show ip interface

Use the **show ip interface** privileged EXEC command to display a list of IP interfaces configured on the device.

Syntax

show ip interface [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*]

- **ethernet** *interface*—An ethernet port. The full syntax is: *unit/port*.
- **vlan** *vlan-id*—VLAN number
- **port-channel** *port-channel-number*—A port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays VLAN 1 configuration.

```
Console# show ip interface vlan 1

Internet address is 10.7.1.192/24

Directed broadcast forwarding is disabled

Proxy ARP is disabled (Global configuration)
```

---

arp

Use the **arp** global configuration command to add a static entry in the Address Resolution Protocol (ARP) cache. To remove an entry from the ARP cache, use the **no** form of this command.

Syntax

arp *ip_addr hw_addr* {**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*}

no arp *ip_addr* {**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*}

- *ip_addr*—IP address or IP alias to map to the specified MAC address.

- *hw_addr*—MAC address to map to the specified IP address or IP alias.
- **ethernet** *interface-number*—Ethernet port number.
- **vlan** *vlan-id*—VLAN number**.**
- **port-channel** *number*—Port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses. Because most hosts support dynamic resolution, static ARP cache entries do not need to be specified.

Examples

The following example adds an IP address and MAC address to the ARP table.

```
Console (config)# arp 198.133.219.232 00-00-0c-40-0f-bc
```

---

arp timeout

Use the **arp timeout** global configuration command to configure how long an entry remains in the ARP cache. To restore the default value, use the **no** form of this command.

Note: The ARP entry is deleted between the period of the "timeout value" and twice the "timeout value". For example, if the timeout value is 20 seconds, the ARP value is deleted during the period of 20 to 40 seconds.

Syntax

arp timeout *seconds*

no arp timeout *seconds*

- *seconds*—Time (in seconds) that an entry remains in the ARP cache. It is recommended not to set the time less than 3600 seconds. A value of zero means that entries are never cleared from the cache (Range: **0-40000000**).

Default Configuration

The default timeout is **60000** seconds.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example configures ARP timeout to 12000 seconds.

```
Console# arp timeout 12000
```

---

clear arp-cache

Use the **clear arp-cache** privileged EXEC command to delete all dynamic entries from the ARP cache.

Syntax

clear arp-cache

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example deletes all dynamic entries from the ARP cache.

```
Console# clear arp-cache
```

---

show arp

Use the **show arp** privileged EXEC command to display entries in the ARP table.

Syntax

show arp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays entries in the ARP table.

```
Console# show arp

Interface IP address HW address Status

---- ---------- ----------------- -------

1/1 10.7.1.102 00:10:B5:04:DB:4B Dynamic

2/2 10.7.1.135 00:50:22:00:2A:A4 Static
```

Back to Contents Page

Back to Contents Page

LACP Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- lacp system-priority
- lacp port-priority
- lacp timeout
- show lacp ethernet
- show lacp port-channel

---

lacp system-priority

Use the **lacp system-priority** global configuration command to configure the system priority. To reset the default value, use the **no** form of this command.

Syntax

lacp system-priority *value*

no lacp system-priority

- *value*—Priority value (Range: **1-65535**).

Default Configuration

The default system priority value is **1**.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the system priority.

```
Console (config)# lacp system-priority 120
```

---

lacp port-priority

Use the **lacp port-priority** interface configuration command to configure the priority value for physical ports. To reset to default priority value, use the **no** form of this command.

Syntax

lacp port-priority *value*

no lacp port-priority

- *value*—Port priority value (Range: **1-65535**).

Default Configuration

The default port priority value is **1**.

Command Mode

Interface Configuration (Ethernet) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the priority value for port 1/e8.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# lacp port-priority 247
```

---

lacp timeout

Use the **lacp timeout** interface configuration command to assign an administrative LACP timeout. To reset the default administrative LACP timeout, use the **no** form of this command.

Syntax

lacp timeout {**long** | **short**}

no lacp timeout

- **long**—Specifies a long timeout value.
- **short**—Specifies a short timeout value.

Default Configuration

The default port timeout value is **long**.

Command Mode

Interface Configuration (Ethernet) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example assigns an administrative LACP timeout for port 1/e8.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# lacp timeout long
```

---

show lacp ethernet

The **show interfaces lacp** privileged EXEC command displays LACP information for ethernet ports.

Syntax

show lacp ethernet *interface*

- *interface*—Ethernet interface

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays LACP statistics information.

```
Console# show lacp ethernet 1/e1 statistics

Port 1/e1 LACP Statistics:

LACP PDUs sent:2



LACP PDUs received:2
```

---

show lacp port-channel

Use the **show lacp port-channel** privileged EXEC command to display LACP information for a port-channel.

Syntax

show lacp port-channel [*port_channel_number*]

- *port_channel_number*—The port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays LACP port-channel information.

```
Console# show lacp port-channel 1

Port-Channel 1:Port Type 1000 Ethernet

Actor

System Priority:1

MAC Address: 000285:0E1C00

Admin Key: 29

Oper Key: 29


Partner

System Priority:0

MAC Address: 000000:000000

Oper Key: 14
```

Back to Contents Page

Back to Contents Page

Line Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- line
- speed
- exec-timeout
- show line

---

line

Use the **line** global configuration command to identify a specific line for configuration and enters the line configuration command mode.

Syntax

line {**console** | **telnet** | **ssh**}

- **console**—Console terminal line.
- **telnet**—Virtual terminal for remote console access (Telnet).
- **ssh**—Virtual terminal for secured remote console access (SSH).

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example configures the device as a virtual terminal for remote console access.

```
Console(config)# line telnet


Console(config-line)#
```

---

speed

The **speed** line configuration command sets the line baud rate. To restore the default setting, use the **no** form of this command.

Syntax

speed {*bps* | **autobaud**}

no speed

- *bps*—Baud rate in bits per second (bps). The options are 2400, 9600, 19200, 38400, 57600 and 115200.
- **autobaud**—Automatic speed synchronization.

Default Configuration

This default speed is autobaud.

Command Mode

Line Configuration (console) Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example sets the baud rate.

```
Console (config)# line console

Console(config-line)# speed 115200
```

---

exec-timeout

The **exec-timeout** line configuration command configures the interval that the system waits until user input is detected. To remove the interval definition, use the **no** form of this command.

Syntax

exec-timeout *minutes* [*seconds*]

no exec-timeout

- *minutes*—Integer that specifies the number of minutes (Range: **0-65535**).
- *seconds*—Additional time intervals in seconds (Range: **0-59**).

Default Configuration

The default configuration is **10** minutes.

Command Mode

Line Configuration Mode

User Guidelines

To specify no timeout, enter the **exec-timeout 0 0** command.

Examples

The following example configures the interval that the system waits until user input is detected at 20 minutes.

```
Console (config)# line console

Console(config-line)# exec-timeout 20
```

---

show line

Use the **show line** user EXEC command to display line parameters.

Syntax

show line [**console** | **telnet** | **ssh**]

- **console**—Console terminal line.
- **telnet**—Virtual terminal for remote console access (Telnet).
- **ssh**—Virtual terminal for secured remote console access (SSH).

Default Configuration

This command has no default configuration.

Command Mode

User EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the line configuration.

```
Console # show line


Console configuration:
Interactive timeout: Disabled
History: 10
Baudrate: 9600
Databits: 8
Parity: none
Stopbits: 1




Telnet configuration:
Interactive timeout: 600
History: 10



SSH configuration:
Interactive timeout: 600
History: 10
```

Back to Contents Page

Back to Contents Page

Management ACL

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- management access-list
- permit (management)
- deny (management)
- management access-class
- show management access-list
- show management access-class

---

management access-list

Use the **management access-list** configuration command to define an access-list for management and enter the access-list context for configuration. If you re-enter the command, all the access-list rules for the existing access-list are implicitly removed. Once in the access-list configuration mode, the denied or permitted access conditions are configured with the **deny** and **permit** commands. To remove an access list, use the **no** form of this command.

Syntax

management access-list *name*

no management access-list *name*

- *name*—The access list name using up to 32 characters.

Default Configuration

This command has no default configuration.

Command Mode

Management Access-list Configuration Mode

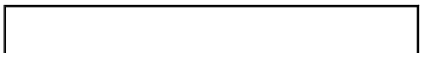
User Guidelines

Use the **management access-class** command to select which access-list is active.

The active access-list cannot be updated or removed.

Examples

The following example shows how to create an access-list, configure two management interfaces, and make the access-list the active list.



```
Console (config)# management access-list mlist

Console (config-macl)# permit ethernet 1/e1

Console (config-macl)# permit ethernet 2/e9

Console (config-macl)# exit

Console (config)# management access-class mlist
```

The following example shows how to create an access-list, configure all interfaces to be management interfaces except interfaces ethernet 1/e1 and ethernet 2/e9, and make the access-list the active list.

```
Console (config)# management access-list mlist

Console (config-macl)# deny ethernet 1/e1

Console (config-macl)# deny ethernet 2/e9

Console (config-macl)# permit

Console (config-macl)# exit

Console (config)# management access-class mlist
```

---

permit (management)

Use the **permit** management access-list configuration command to define a permit rule.

Syntax

permit [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*] [**service** *service*]

permit ip-source *ip-address* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*] [**service** *service*]

- **ethernet** *interface-number*—An ethernet port number.
- **vlan** *vlan-id*—A VLAN number.
- **port-channel** *number*—A port-channel number.
- *ip-address*—Source IP address.
- **mask** *mask*—Specifies the network mask of the source IP address.
- **mask** *prefix-length*—Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/).
- **service** *service*—Indicates service type. Can be one of the following service types: **telnet**, **ssh**, **http, https** or **snmp**.

Default Configuration

This command has no default configuration.

Command Mode

Management Access-list Configuration Mode

User Guidelines

Where no parameters are entered, all ports are automatically configured as permitted.

Examples

The following example permits all ports in the access-list called `mlist`.

```
Console (config)# management access-list mlist

Console (config-macl)# permit
```

---

deny (management)

Use the **deny** management access-list configuration command to define a deny rule.

Syntax

deny [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*] [**service** *service*]

deny ip-source *ip-address* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*] [**service** *service*]

- **ethernet** *interface-number*—An ethernet port number.
- **vlan** *vlan-id*—A VLAN number.
- **port-channel** *number*—A port-channel number.
- *ip-address*—Source IP address.
- **mask** *mask*—Specifies the network mask of the source IP address.
- **mask** *prefix-length*—Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/).
- **service** *service*—Indicates service type. Can be one of the following: **telnet**, **ssh**, **http, https** or **snmp**.

Default Configuration

This command has no default configuration.

Command Mode

Management Access-list Configuration Mode

User Guidelines

Where no parameters are entered, all ports are automatically configured as denied.

Examples

The following example denies all ports in the access-list.

```
Console (config)# management access-list mlist

Console (config-macl)# deny
```

---

management access-class

Use the **management access-class** global configuration command to define which management access-list is used. To disable the restrictions, use the **no** form of this command.

Syntax

management access-class {**console-only** | *name*}

no management access-class

- *name*—An access-list name. If unspecified, defaults to an empty access-list.
- **console-only**—The device can be managed only from the console.

Default Configuration

The default is no restictions.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example configures an access-list as the management access-list.

```
Console (config)# management access-class mlist
```

---

show management access-list

Use the **show management access-list** privileged EXEC command to display management access-lists.

Syntax

show management access-list [*name*]

- *name*—An access-list name.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the active management access-list.

```
Console# show management access-list

mlist
```

```
-----

permit ethernet 1/e1

permit ethernet 2/e9

! (Note: all other access implicitly denied)
```

---

show management access-class

Use the **show management access-class** user EXEC command to display the active management access-list.

Syntax

show management access-class

Default Configuration

This command has no default configuration.

Command Mode

User EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the management access-list information.

```
Console> show management access-class

Management access-class is enabled, using access list mlist
```

Back to Contents Page

Back to Contents Page

Port Channel Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- interface port-channel
- interface range port-channel
- channel-group
- show interfaces port-channel

---

interface port-channel

Use the **interface port-channel** global configuration command to enter the interface configuration mode of a specific port-channel.

Syntax

interface port-channel *port-channel-number*

- *port-channel-number*—A port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters the context of port-channel number 1.

```
Console (config)# interface port-channel 1
```

---

interface range port-channel

Use the **interface range port-channel** global configuration command to enter the interface configuration mode to configure multiple port channels.

Syntax

interface range port-channel {*port-channel-range* | **all**}

- *port-channel-range*—List of port-channels to configure. Separate non-consecutive port-channels with a comma and no spaces. A hyphen designates a range of port-channels.
- **all**—All the channel-ports

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

Commands under the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, it stops the execution of the command on subsequent interfaces.

Example

The following example groups port-channel 1, 2, and 6 to receive the same command.

```
Console(config)# interface range port-channel 1-2, 6

Console(config-if)#
```

---

channel-group

The **channel-group** interface configuration command associates a port with a port-channel. To remove a port from a port-channel, use the **no** form of this command.

Syntax

channel-group *port-channel-number* **mode** {**on** | **auto**}

no channel-group

- *port_channel_number*—The port-channel number for the current port to join.
- **on**—Forces the port to join a channel.
- **auto**—Allows the port to join a channel as a result of an LACP operation.

Default Configuration

The port is not assigned to any port-channel.

Command Mode

Interface Configuration (Ethernet) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures port 1/e5 to port-channel number 1 without LACP.

```
(config)# interface ethernet 1/e5

(config-if)# channel-group 1 mode on
```

---

show interfaces port-channel

Use the **show interfaces port-channel** privileged EXEC command to display port-channel information (which ports are members of that port-channel, and whether they are currently active or not).

Syntax

show interfaces port-channel [*port-channel-number*]

- *port_channel_number*—The port-channel to display.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all port-channel information.

```
Console # show interfaces port-channel

Channel Port

------------ ---------------------------------

1 Active 1/e1, 2/e2 Inactive 3/e3

2 Active 1/e2

3 Inactive 3/e8
```

Back to Contents Page

Back to Contents Page

Port Monitor Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- port monitor
- show ports monitor

---

port monitor

Use the **port monitor** interface configuration command to start a port monitoring session. To stop a port monitoring session, use the **no** form of this command.

Syntax

port monitor *src-interface* [**rx** | **tx**]

no port copy *src-interface*

- *src-interface*—Valid ethernet port or port-channel number.
- **rx**—Monitors only received packets. If no option is specified, both rx and tx packets are received.
- **tx**—Monitors only transmitted packets. If no option is specified, both Rx and Tx packets are received.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet) Mode

User Guidelines

This command enables traffic on one port to be copied to another port, or between the source port (src-interface) and a destination port (the port being configured).

The port being monitored cannot be set faster than the monitoring port.

The following restrictions apply to ports configured to be destination ports:

- The port cannot be already configured as a source port.
- The port cannot be a member of a port-channel.
- An IP interface is not configured on the port.
- GVRP is not enabled on the port.
- The port is not a member in any VLAN, except for the default VLAN (will automatically removed from the default VLAN).

The following restrictions apply to ports configured to be source ports:

- Port monitoring source ports must be simple ports, and not port-channel ports
- The port cannot be already configured as a destination port.
- All the frames are transmitted already tagged from the destination port.
- There is no limitation on the number of source ports, but only one destination port can be defined.

Example

The following example copies traffic on port 1/e8 (source port) to port 1/e1 (destination port).

```
Console(config)# interface ethernet 1/e1

Console(config-if)# port monitor 1/e8
```

---

show ports monitor

Use the **show ports monitor** privileged EXEC command to display the port monitoring status.

Syntax

show ports monitor

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the device port copy status.

```
Console# show ports monitor
```

```
Source port Destination Port Type Status

----------- ---------------- ----- -------

1/e1 1/e8 RX, TX Active

1/e2 1/e8 RX Active
```

Back to Contents Page

Back to Contents Page

QoS Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- ip access-list
- permit (IP)
- deny (IP)
- mac access-list
- permit (MAC)
- deny (MAC)
- service-acl
- show access-lists
- show interfaces access-lists
- qos
- show qos
- wrr-queue cos-map
- wrr-queue bandwidth
- priority-queue out num-of-queues
- show qos interface
- qos map dscp-queue
- qos trust(Global)
- qos trust(Interface)
- qos cos
- qos map tcp-port-queue
- qos map udp-port-queue
- show qos map

---

ip access-list

Use the **ip access-list** global configuration command to create Layer 3 ACLs and enter IP-access list configuration Mode. To delete an IP ACL, use the **no** form of this command.

Syntax

ip access-list *name*

no ip access-list *name*

- *name*—Enter the IP ACL name.

Default Configuration

The default is deny-all.

Command Mode

Global Configuration Mode

User Guidelines

The **ip-access-list** command enters the IP-access list configuration mode.

Example

The following example creates an ACL named Dell.

```
```

```
Console (config)# ip-access-list Dell
```

---

permit (IP)

Use the **permit ip** access-list configuration mode command to allow traffic if the conditions defined in the permit statement are matched.

Syntax

permit {**any** | *protocol*} {**any** | {*source source-wildcard*}} {**any** | {*destination destination-wildcard*}} [**dscp** *dscp number* | **ip-precedence** *ip-precedence*]

permit-tcp {**any** | *source source-wildcard*}} {**any** | *source-port*} {**any** | *destination destination-wildcard*}} {**any** | *destination-port*} [**dscp** *dscp number* | **ip-precedence** *ip-precedence*]

permit-udp {**any** | {*source source-mask*}} {**any** | *source-port*} {**any** | {*destination destination-mask*}}{**any**|*destination-port*} [**dscp** *dscp number* | **ip-precedence** *ip-precedence*]

- Source IP address can be one of the following:
  - **any**—Packets received from any MAC address.
  - *source source-wildcard*—IP address and wildcard for host from which the packet is sent. Specify the IP address as 0.0.0.0 and mask as 255.255.255.255.
- Destination IP address can be one of the following:
  - **any**—Packets sent to any IP address.
  - *destination destination-wildcard*—IP address and wildcard for host to which the packet is sent. Specify the IP address as 0.0.0.0 and mask as 255.255.255.255.
- *protocol*—The name or the number of an IP protocol. Use ? to see list of available protocols (**icmp**, **igmp**, **ip**, **tcp**, **egp**, **igp**, **udp**, **hmp**, **rdp**, **idpr**, **ipv6**, **ipv6-route**, **ipv6-frag**, **idrp**, **rsvp**, **gre**, **esp**, **ah**, **ipv6-icmp**, **eigrp**, **ospf**, **ipip**, **pim**, **l2tp**, **isis**), use **any** for all protocols.
- *destination-port*—Specifies the UDP/TCP destination port. Use **any** for all ports.
- *source-port*—Specifies the UDP/TCP source port. Use **any** for all ports.
- **dscp**—Matches *dscp number* with the packet DSCP value.
- **precedence**—Matches *ip-precedence* with the packet ip-precedence value.

Default Configuration

This command has no default configuration.

Command Mode

IP Access-List Configuration Mode

User Guidelines

The matching criteria in IP-ACLs are defined in ACEs. The ACE is defined using the permit (IP) or deny (IP) command. Up to 256 ACEs are combined into an IP-ACL.

If there are no matches, the packets are denied.

Example

The following example creates an ACE allowing RSVP protocol traffic from 12.1.1.1 with DSCP 56.

```
Console (config-ip-al)# permit rsvp 12.1.1.1 0.0.0.0 any dscp 56
```

---

deny (IP)

Use the **deny** IP access-list configuration command to deny traffic if the conditions defined in the deny statement are matched.

Syntax

deny [**disable-port**] {**any** | *protocol*} {**any** | {*source source-wildcard*}} {**any** | {*destination destination-wildcard*}} [**dscp** *dscp number* | **ip-precedence** *ip-precedence*]

deny-tcp [**disable-port**] {**any** | {*source source-wildcard*}} {**any** |*source-port*} {**any** | {*destination destination-wildcard*}} {**any** |*destination-port*} [**dscp** *dscp number* | **ip-precedence** *ip-precedence*]

deny-udp [**disable-port**] {**any** | {*source source-mask*}} {**any** | *source-port*} {**any** | {*destination destination-mask*}} {**any** | *destination-port*} [**dscp** *dscp number* | **ip-precedence** *ip-precedence*]

- **disable-port**—if the statement is deny, then the port is disabled.
- Source IP address can be one of the following:
  - **any**—Packets received from any MAC address.
  - *source source-wildcard*—IP address and wildcard for host from which the packet is sent. Specify the IP address as 0.0.0.0 and mask as 255.255.255.255.
- Destination IP address can be one of the following:
  - **any**—Packets sent to any IP address.
  - *destination destination-wildcard*—IP address and wildcard for host to which the packet is sent. Specify the IP address as 0.0.0.0 and mask as 255.255.255.255.
- *protocol*—The name or the number of an IP protocol. Use ? to see a list of available protocols (**icmp**, **igmp**, **ip**, **tcp**, **egp**, **igp**, **udp**, **hmp**, **rdp**, **idpr**, **ipv6**, **ipv6-route**, **ipv6-frag**, **idrp**, **rsvp**, **gre**, **esp**, **ah**, **ipv6-icmp**, **eigrp**, **ospf**, **ipip**, **pim**, **l2tp**, **isis**) use **any** for all protocols
- *destination-port*—Specifies the UDP/TCP destination port. Use **any** for all ports.
- *source-port*—Specifies the UDP/TCP source port. Use **any** for all ports.
- **dscp**—Matches *dscp number* with the packet DSCP value.
- precedence—Matches *ip-precedence* with the packet ip-precedence value.

Default Configuration

This command has no default configuration.

Command Mode

IP Access-List Configuration Mode

User Guidelines

The matching criteria in IP-ACLs are defined in ACEs. The ACE is defined using the permit (IP) or deny (IP) command. Up to 248 ACE's are combined into an IP-ACL.

If there are no matches, the packets are denied.

Example

The following example creates an ACE denying any IP traffic from address `192.1.1.10` with wildcard `0.0.0.255` or traffic to `192.168.1.10` with the mask `255.255.255.0`.

```
Console (config-ip-al)# deny any 192.1.1.10 0.0.0.255 192.168.1.10 255.255.255.0
```

---

mac access-list

Use the **mac access-list** global configuration command to create Layer 2 MAC ACLs and enter the MAC-Access list configuration mode. To delete a MAC ACL, use the **no** form of this command.

Syntax

mac access-list *name*

no mac access-list *name*

- *name*—Enter the IP ACL name consisting of a character string up to 32 characters long.

Default Configuration

The default for all ACLs is **deny**.

Command Mode

Global Configuration Mode

User Guidelines

Entering the **mac access-list** command enables the MAC-access list configuration mode.

Example

The following example creates a MAC ACL named `dell`.

```
Console (config)# mac access-list dell
```

---

permit (MAC)

Use the **permit** extended mac-list configuration mode command to allow traffic if the conditions defined in the permit statement are matched.

Syntax

permit {**any** | {host *source source-wildcard*} **any** | {*destination destination-wildcard*}}[**vlan** *vlan-id*]

- Source MAC address can be one of the following:
  - **any**—Packets received from any MAC address.
  - *source source-wildcard*—MAC address and wildcard for host from which the packet is sent. Specify the MAC address and wildcard using hexadecimal format (HH:HH:HH:HH:HH:HH).
- Destination MAC address can be one of the following:
  - **any**—Packets sent to any MAC address.
  - *destination destination-wildcard*—MAC address and wildcard for host to which the packet is sent. Specify the MAC address and wildcard using hexadecimal format (HH:HH:HH:HH:HH:HH).
- **vlan** *vlan-id*—The packet VLAN.

Default Configuration

This command has no default configuration.

Command Mode

MAC-List Configuration Mode

User Guidelines

The matching criteria in MAC-ACLs are defined in ACEs.

Example

The following example creates a MAC ACE that allows traffic from MAC address 6:6:6:6:6:6 with any destination on VLAN 4.

```
Console (config-mac-al)# permit 6:6:6:6:6:6 0:0:0:0:0:0 any vlan 4
```

---

deny (MAC)

Use the **deny** extended mac-list configuration mode command to allow traffic if the conditions defined in the permit statement are matched.

Syntax

deny [**disable-port**] {**any** | {*source source-wildcard*} **any** | {*destination destination-wildcard*}} [**vlan** *vlan-id*]

- **disable-port**—If the statement is deny, then the port is disabled.
- Source MAC address can be one of the following:
  - **any**—Packets received from any MAC address.
  - *source source-wildcard*—MAC address and wildcard for host from which the packet is sent. Specify the MAC address and wildcard using hexadecimal format (HH:HH:HH:HH:HH:HH).
- Destination MAC address can be one of the following:
  - **any**—Packets sent to any MAC address.
  - *destination destination-wildcard*—MAC address and wildcard for host to which the packet is sent. Specify the MAC address and wildcard using hexadecimal format (HH:HH:HH:HH:HH:HH).
- **vlan** *vlan-id*—The packet VLAN.

Default Configuration

This command has no default configuration.

Command Mode

Extended MAC-List Configuration Mode

User Guidelines

The matching criteria in MAC-ACLs are defined in ACEs.

Example

The following example creates a MAC ACE that denies traffic from MAC address 6:6:6:6:6:6.

```
Console (config-mac-al)# deny 6:6:6:6:6:6 0:0:255:255:255:255
```

---

service-acl

Use the **service-acl** interface configuration command to apply an access-list to the interface input. To detach an access-list from an interface, use the **no** form of this command.

Syntax

service-acl {**input** *acl-name* | **output** *acl -map-name*}

no service-acl {**input** | **output**}

- **input** *acl-name*—Applies the specified ACL to the input interface.
- **output** *acl-name*—Applies the specified ACL to the output interface.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, VLAN, port-channel) Mode

User Guidelines

Only one ACL per interface per direction is supported.

Example

The following example attaches the ACL named dell to the interface input.

```
Console (config-if)# service acl input dell
```

---

show access-lists

Use the **show access-lists** privileged EXEC command to display access control lists (ACLs) defined on the device.

Syntax

show access-lists [*name*]

- *name*—The ACL name.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays access control lists (ACLs) configured on the device.

```
Console # show access-lists

IP access list ACL1

permit 234 172.30.40.1 0.0.0.0 any

permit 234 172.30.8.8 0.0.0.0 any
```

---

show interfaces access-lists

Use the **show interfaces access-lists** privileged EXEC command to display access lists applied on interfaces.

show interfaces access-lists [**ethernet** *interface* | **vlan** *vlan-id* | **port-channel** *port-channel-number*]

- *interface*—The full syntax is: *unit*/*port*.
- *vlan-id*—VLAN number
- *port-channel-number*—Port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays access control lists (ACLs) configured on the device.

```
Console# show interfaces access-lists

Interface Input ACL

--------- ----------

1/1 ACL1

2/1 ACL3
```

---

qos

Use the **qos** global configuration command to enable quality of service (QoS) on the device. To disable the QoS features on the device, use the **no** form of this command.

Syntax

qos

no qos

Default Configuration

The default QoS value is enabled.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables QoS on the device.

```
```

```
Console (config)# qos
```

---

show qos

Use the **show qos** user EXEC command to display the QoS activity status.

Syntax

show qos

Default Configuration

This command has no default configuration.

Command Mode

User EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays a device QoS status.

```
Console>show qos

Qos: disable

Trust: dscp
```

---

wrr-queue cos-map

Use the **wrr-queue cos-map** global configuration command to map assigned CoS values to the egress queues. To return to the default values, use the **no** form of this command.

Syntax

wrr-queue cos-map *queue-id cos1…cos*n

no wrr-queue cos-map {*queue-id*}

- queue-id—The queue number to which the following CoS values are mapped.
- *cos1…cos*n—Map to specific queues up to eight CoS values from 1 to 7.

Default Configuration

Default values for three queues are as follows:

- CoS value 1 select queue 1
- CoS value 2 select queue 1
- CoS value 0 select queue 2
- CoS value 3 select queue 2
- CoS value 4 select queue 2
- CoS value 5 select queue 3
- CoS value 6 select queue 3
- CoS value 7 select queue 3

Command Mode

Global Configuration Mode

User Guidelines

This command is used to distribute traffic into different queues, where each queue is configured with different weighted round robin (WRR) and weighted random early detection (WRED) parameters.

Queues are enabled by using the priority-queue out num-of-queues interface configuration command.

Example

The following example maps CoS 2 to queue 4.

```
Console (config)# wrr-queue cos-map 4 2
```

---

wrr-queue bandwidth

Use the **wrr-queue bandwidth** global configuration command to assign weighted round robin (WRR) weights to egress queues. The weights ratio determines the frequency in which the packet scheduler dequeues packets from each queue. To return to the default values use, the **no** form of this command.

Syntax

wrr-queue bandwidth *weight1 weight2 ... weight_n*

no wrr-queue bandwidth

- *weight1... weight_n*—Sets the frequency ratio in which the WRR packet scheduler dequeues packets. Separate each value by spaces (Range: **1 - 65535**).

Default Configuration

The default WRR weight is 1/4 ratio for all queues (each weight is set to 1).

Command Mode

Global Configuration Mode

User Guidelines

The ratio is calculated and managed as follows:

The ratio for each queue is defined by the queue weight divided by the sum of all queue weights (that is, the normalized weight). This sets the ratio of the frequency in which the WRR packet scheduler dequeues packets, and not the bandwidth. Thus, the ratio will be of the number of packets and not bytes sent from each queue.

A weight of 0 means no bandwidth is allocated for the same queue, and the share bandwidth is divided among the remaining queues.

Example

The following example sets queue weights as follows:

- Queue 1—10/100
- Queue 2—20/100
- Queue 3—30/100
- Queue 4—40/100

```
Console (config)# wrr-queue bandwidth 10 20 30 40
```

---

priority-queue out num-of-queues

Use the **priority-queue out num-of-queues** global configuration command to enable the egress queues to be strict priority (Expedite) queues. To set all queues to strict priority (Expedite) queues, use the **no** form of this command. **EF** refers to expedite

Syntax

priority-queue out num-of-queues [*number-of-queues*]

no priority-queue out num-of-queues

- *number-of-queue*—Assigns the number of queues to be strict priority (Expedite) queues. The strict priority (Expedite) queues are the queues with higher indexes. The range is 0 – 4.

Default Configuration

All queues are strict priority (Expedite) queues.

Command Mode

Global Configuration Mode

User Guidelines

When configuring the **priority-queue out num-of-queues** command, the weighted round robin (WRR) weight ratios are affected because there are fewer queues participating in WRR. This means that corresponding weight in the wrr-queue bandwidth command is ignored (not used in the ratio calculation).

Example

The following example sets queues 3, 4 to be EF queues.

```
Console (config)# priority-queue out num-of-queues 2
```

---

show qos interface

Use the **show qos interface** user EXEC command to display interface QoS data. **EF** refers to expedite

Syntax

show qos interface [**ethernet** *interface-number* | **port-channel** *number*] [**queuing**]

- **ethernet** *interface-number*—Ethernet port number
- **port-channel** *number*—Port channel number
- **queuing**—Display the queue strategy (WRR or EF) and the weight for WRR queues and the CoS to queue map and the EF priority.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

If no keyword is specified with the **show qos interface** command, the port QoS mode trusted, untrusted, and default CoS values are displayed. If a specific interface is not specified, the information for all interfaces is displayed.

Example

The following example displays the output from the **show qos interface ethernet** 1/e5 **queueing** command for 4 queues.

```
Console> show qos interface ethernet 1/e5 queueing

Ethernet 1/e5

wrr bandwidth weights and EF priority:

qid-weights Ef - Priority

1 — 125 dis- N/A

2 — 125 dis- N/A

3 — 125 dis- N/A

4 — 125 dis- N/A

Cos-queue map:

cos-qid

0 - 2

1 - 1

2 - 1

3 - 2

4 - 3
```

```
5 - 3


6 - 4


7 - 4
```

---

qos map dscp-queue

Use the **qos map dscp-queue** global configuration command to modify the DSCP to CoS map. To return to the default map, use the **no** form of this command.

Syntax

qos map dscp-queue *dscp-list* to *queue-id*

no qos map dscp-queue

- *dscp-list*—Specify 4 DSCP values, separate each DSCP with a space (Range: **0-63**).
- *queue-id*—Enter the queue number to which the DSCP value corresponds.

Default Configuration

The following table describes default map.

DSCP value	0-15	16-39	40-63
Queue-ID	1	2	3

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example maps DSCP values 33, 40, and 41 to queue 1.

```
Console (config)# qos map dscp-queue 33 40 41 to 1
```

---

qos trust(Global)

Use the **qos trust** global configuration command to configure the system trust state. To return to the untrusted state, use the **no** form of this command.

Syntax

qos trust cos | dscp | tcp-udp-port

no qos trust

- **cos**—Classifies ingress packets with the packet CoS values. For untagged packets, the port default CoS is used.
- **dscp**—Classifies ingress packets with the packet DSCP values.
- **tcp-udp-port to dscp**—Classifies ingress packets with the packet destination port values.

Default Configuration

The default trust mode is CoS.

Command Mode

Global Configuration Mode

User Guidelines

Packets entering a quality of service (QoS) domain are classified at the edge of the QoS domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain.

Use this command to specify whether the port is trusted and to specify which packet fields to use to classify traffic.

If DSCP is trusted, the DSCP field of the IP packet is not modified.

If TCP-UDP-port is trusted then the packet destination port is not modified.

If CoS is trusted, CoS or the packet is not modified.

Example

The following example configures the system to the trust state.

```
Console (config)# qos trust dscp
```

qos trust(Interface)

Use the **qos trust** interface configuration command to enable each port trust state. To disable the trust state on each port use the no form of this command.

Syntax

qos trust

no qos trust

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures port 1/e5 to the trust state.

```
Console (config)# interface ethernet 1/e5

Console (config-if)# qos trust
```

---

qos cos

Use the **qos cos** interface configuration command to configure the default port CoS value. To return to the default setting, use the **no** form of this command.

Syntax

qos cos *default-cos*

no qos cos *default-cos*

- *default-cos*—Specifies the default CoS value assigned to the port. If the port is trusted and the packet is untagged, then the default CoS value becomes the CoS value (Range: **0-7**).

Default Configuration

Port CoS value is 0.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

The default value assigns a CoS value to all untagged packets entering the port.

Example

The following example configures port 1/e5 default CoS value to 3.

```
Console (config)# interface ethernet 1/e5

Console (config-if)# qos cos 3
```

---

qos map tcp-port-queue

Use the **qos map tcp-port-queue** global configuration command to modify the TCP-Port to DSCP table. To delete table entries use the **no** form of this command. When there are no entries to delete and the **no** form of this command is used, the entire table is deleted.

Syntax

qos map tcp-port-dscp *port1...port8* to *queue-id*

no qos map tcp-port-dscp [*port1...port8*]

- *port1...port8*—Specifies up to 8 ports (destination ports) separated by commas that are being mapped (Range: **0-65535**).
- *queue-id*—Specifies the queue number being mapped.

Default Configuration

The table is empty.

Command Mode

Global Configuration Mode

User Guidelines

This command maps the TCP destination port in the ingress packet to a specified queue.

This map is used when the TCP trust mode is enabled and when trust command is enabled.

Example

The following example modifies the mapped TCP ports 2000 and 80 to queue 2.

```
Console (config)# qos map tcp-port-queue 2000 80 to 2
```

---

qos map udp-port-queue

Use the **qos map udp-port-queue** global configuration command to modify the UDP-Port to DSCP table. To delete table entries, use the **no** form of this command. When there are no entries to delete and the **no** form of this command is used, the entire table is deleted.

Syntax

qos map udp-port-dscp *port1...port8 to queue-id*

no qos map udp-port-dscp [*port1...port8*]

- *port1...port8*—Specify up to 8 ports (destination ports) separated by commas that are being mapped (Range: **0-65535**).
- *queue-id*—Specify the queue number being mapped.

Default Configuration

The table is empty.

Command Mode

Global Configuration Mode

User Guidelines

This command maps the UDP destination port in the ingress packet to a specified queue.

This map is used when the UDP trust mode is enabled and when the **trust** command is enabled.

Example

The following example modifies the mapped UDP ports 2000 and 80 to queue 2.

```
Console (config)# qos map udp-port-queue 2000 80 to 2
```

---

show qos map

Use the **show qos map** user EXEC command to display all the QoS maps.

Syntax

show qos map [**dscp-queue** | **tcp-port-queue** | **udp-port-queue**

- **dscp-queue**—Displays the DSCP to queue map.
- **tcp-port-queue**—Displays the TCP Port to queue map.
- **udp-port-queue**—Displays the UDP Port to queue map.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC command

User Guidelines

There are no user guidelines for this command.

The following example displays the DSCP queue map.

```
 Dscp-queue map:


d1 : d2 0 1 2 3 4 5 6 7 8 9


-----------------------------------
```

```
0 : 01 01 01 01 01 01 01 01 01 01

1 : 01 01 01 01 01 01 02 02 02 02

2 : 02 02 02 02 02 02 02 02 02 02

3 : 02 02 03 03 03 03 03 03 03 03

4 : 03 03 03 03 03 03 03 03 04 04

5 : 04 04 04 04 04 04 04 04 04 04

6 : 04 04 04 04
```

The following table appears if **tcp-port-queue** is supported.

```
Tcp port-queue map:

Port queue

----- ------

6000 1

6001 2

6002 3
```

Back to Contents Page

Back to Contents Page

Radius Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- radius-server host
- radius-server key
- radius-server retransmit
- radius-server source-ip
- radius-server timeout
- radius-server deadtime
- show radius-servers

---

radius-server host

Use the **radius-server host** global configuration command to specify a RADIUS server host. To delete the specified RADIUS host, use the **no** form of this command.

Syntax

radius-server host *ip-address* [**auth-port** *auth-port-number*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *deadtime*] [**key** *key-string*] [**source** *source*] [**priority** *priority*]

no radius-server host *ip-address*

- *ip-address*—The RADIUS server host IP address.
- *auth-port-number*—Port number for authentication requests. The host is not used for authentication if set to 0. If unspecified, the port number defaults to **1645** (Range: **0-65535**).
- *timeout*—Specifies the timeout value in seconds. If no timeout value is specified, the global value is used (Range: **1-30**).
- *retries*—Specifies the re-transmit value. If no re-transmit value is specified, the global value is used (Range: **1-10**).
- *deadtime*—Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests (Range **0-2000**).
- *key-string*—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. If no key value is specified, the global value is used.
- *source*—Specifies the source IP address to use for the communication. If no retransmit value is specified, the global value is used.
- *priority*—Determines the order in which the servers are used, where 0 is the highest priority (Range: **0-65535**).

Default Configuration

If no RADIUS host is specified, the global **radius-server** command values are used as the default.

Command Mode

Global Configuration Mode

User Guidelines

To specify multiple hosts, multiple **radius-server host** commands can be used.

If no host-specific timeout, retransmit, deadtime or key values are specified, the global values apply to each host.

Examples

The following example specifies a RADIUS server host with the following characteristics:

- Server host IP address—192.168.10.1
- Authentication port number—1256
- Timeout period—20 seconds.

```
Console (config)# radius-server host 192.168.10.1 auth-port 1256 timeout 20
```

---

radius-server key

The **radius-server key** global configuration command sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon. To reset to the default, use the **no** form of this command.

Syntax

radius-server key *key-string*

no radius-server key

- *key-string*—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. The key can be up to 160 characters long.

Default Configuration

The default is an empty string.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon to dell-server.

```
```

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

---

radius-server retransmit

Use the **radius-server retransmit** global configuration command to specify the number of times the software searches the list of RADIUS server hosts. To reset the default configuration, use the **no** form of this command.

Syntax

radius-server retransmit *retries*

no radius-server retransmit

- *retries*—Specifies the retransmit value (Range: **1-10**).

Default Configuration

The default is 3 attempts.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example configures the number of times the software searches the list of RADIUS server hosts (5 attempts).

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

---

radius-server source-ip

Use the **radius-server source-ip** global configuration command to specify the source IP address used for communication with RADIUS servers. To return to the default, use the **no** form of this command.

Syntax

radius-server source-ip *source*

no radius-server-ip

- *source*—Specifies the source IP address.

Default Configuration

The default IP address is the outgoing IP interface.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example configures the source IP address used for communication with RADIUS servers.

```
Console (config)# radius-server source-ip 10.1.1.1
```

---

radius-server timeout

Use the **radius-server timeout** global configuration command to set the interval for which a device waits for a server host to reply. To restore the default, use the **no** form of this command.

Syntax

radius-server timeout *timeout*

no radius-server timeout

- *timeout*—Specifies the timeout value in seconds (Range: **1-30**).

Default Configuration

The default value is **3** seconds.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example sets the interval for which a device waits for a server host to reply.

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

---

radius-server deadtime

Use the **radius-server deadtime** global configuration command to improve RADIUS response times when servers are unavailable. The command is used to cause the unavailable servers to be skipped. To reset the default value, use the **no** form of this command.

Syntax

radius-server deadtime *deadtime*

no radius-server deadtime

- *deadtime*—Length of time in minutes, for which a RADIUS server is skipped over by transaction requests (Range: **0-2000**).

Default Configuration

The default dead time is **0** minutes.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example sets a dead time where a RADIUS server is skipped over by transaction requests.

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

---

show radius-servers

Use the **show radius-servers** privileged EXEC command to display the RADIUS server settings.

Syntax

show radius-servers

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the RADIUS server settings.

```
Console# show radius-servers

Port

IP address Auth Acct TimeOut Retransmit deadtime source IP Priority

---------- ---- ---- ------- ---------- -------- ----------- --------

172.16.1.1 1645 1646 3 3 0 172.16.8.1 1

172.16.1.2 1645 1 646 11 8 0 172.16.8.1 2
```

Back to Contents Page

Back to Contents Page

RMON Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- show rmon statistics
- rmon collection history
- show rmon collection history
- show rmon history
- rmon alarm
- show rmon alarm-table
- show rmon alarm
- rmon event
- show rmon events
- show rmon log
- rmon table-size

---

show rmon statistics

Use the **show rmon statistics** privileged EXEC command to display RMON ethernet statistics.

Syntax

show rmon statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—An ethernet port. The full syntax is: *unit/port*.
- *port-channel-number*—A port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays RMON ethernet statistics for port 1/e1.

```
Console# show rmon statistics ethernet 1/e1

Port 1/e1
```

```
Dropped: 8

Octets: 878128 Packets: 978

Broadcast: 7 Multicast: 1

CRC Align Errors: 0 Collisions: 0

Undersize Pkts: 0 Oversize Pkts: 0

Fragments: 0 Jabbers: 0

64 Octets: 98 65 to 127 Octets: 0

128 to 255 Octets: 0 256 to 511 Octets: 0

512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

The following table describes the significant fields shown in the display:

Field	Description
Dropped	The total number of events in which packets are dropped by the probe due to lack of resources. This number is not always the number of packets dropped; it is the number of times this condition has been detected.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast	The total number of good packets received and directed to the broadcast address. This does not include multicast packets.
Multicast	The total number of good packets received and directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC Align Errors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS), with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize Pkts	The total number of packets received less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.
Oversize Pkts	The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
Fragments	The total number of packets received less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (Alignment Error).
Jabbers	The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	The best estimate of the total number of collisions on this ethernet segment.
64 Octets	The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	The total number of packets (including bad packets) received between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128 to 255 Octets	The total number of packets (including bad packets) received between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256 to 511 Octets	The total number of packets (including bad packets) received between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512 to 1023 Octets	The total number of packets (including bad packets) received that are between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024 to 1518 Octets	The total number of packets (including bad packets) received that are between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

---

rmon collection history

Use the **rmon collection history** interface configuration command to enable a Remote Monitoring (RMON) MIB history statistics group on an interface. To remove a specified RMON history statistics group, use the **no** form of this command.

Syntax

rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

no rmon collection history *index*

- *index*—The requested statistics index group (Range: **1-65535**).
- **owner** *ownername*—Records the RMON statistics group owner name. If unspecified, the name is an empty string.
- **buckets** *bucket-number*—A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50 (Range: **1-65535**).
- **interval** *seconds*—The number of seconds in each polling cycle. If unspecified, defaults to 1800 (Range: **1-3600**).

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

This command cannot be executed on multiple ports using the interface range ethernet command.

Examples

The following example enables a Remote Monitoring (RMON) MIB history statistics group.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# rmon collection history 1 interval 2400
```

---

show rmon collection history

Use the **show rmon collection history** privileged EXEC command to display the requested history group configuration.

Syntax

show rmon collection history [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—An ethernet port. The full syntax is: *unit/port*.
- *port-channel-number*—A port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays all RMON group statistics.

```
Console# show rmon collection history

Index Interface Interval Requested Granted Owner
Samples Samples
----- ----- ---------- ---------- -------- -------
1 1/e1 30 50 50 CLI
2 1/e1 1800 50 50 Manager
```

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the entry.
Interface	The sampled ethernet interface
Interval	The interval in seconds between samples.
Requested Samples	The requested number of samples to be saved.
Granted Samples	The granted number of samples to be saved.
Owner	The entity that configured this entry.

show rmon history

Use the **show rmon history** privileged EXEC command to display RMON ethernet statistics history.

Syntax

show rmon history *index* {**throughput** | **errors | other**} [**period** *seconds*]

- *index*—The requested set of samples (Range: **1-65535**).
- **throughput**—Displays throughput counters.
- **errors**—Displays error counters.
- **other**—Displays drop and collision counters.
- **period** *seconds*—Specifies the requested period time to display (Range: **0–2147483647**).

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays RMON Ethernet Statistics history for throughput on index number 1.

```
Console# show rmon history 1 throughput

Sample set: 1 Owner: CLI

Interface: 1/1 Interval: 1800

Requested samples: 50 Granted samples: 50

Maximum table size: 500

Time Octets Packets Broadcast Multicast Utilization
```

```
-------------------- ---------- --------- --------- ---------- ----

Jan 18 2002 21:57:00 303595962 357568 3289 7287 19.98%

Jan 18 2002 21:57:30 287696304 275686 2789 5878 20.17%
```

The following example displays RMON Ethernet Statistics history for errors on index number 1.

```
Console# show rmon history 1 errors

Sample set: 1 Owner: Me

Interface: 1/1 Interval: 1800

Requested samples: 50 Granted samples: 50

Maximum table size: 500 (800 after reset)

Time CRC Align Undersize Oversize Fragments Jabbers

-------------------- ---------- --------- --------- ---------- ---

Jan 18 2002 21:57:00 1 1 0 49 0

Jan 18 2002 21:57:30 1 1 0 27 0
```

The following example displays RMON Ethernet Statistics history for **other** on index number 1.

```
Console# show rmon history 1 other

Sample set: 1 Owner: Me

Interface: 1/1 Interval: 1800

Requested samples: 50 Granted samples: 50

Maximum table size: 500

Time Dropped Collisions
```

```
-------------------- ------- ----------


Jan 18 2002 21:57:00 3 0


Jan 18 2002 21:57:30 3 0
```

The following table describes the significant fields shown in the display:

Field	Description
Time	Date and time the entry is recorded.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The number of packets (including bad packets) received during this sampling interval.
Broadcast	The number of good packets received during this sampling interval that were directed to the broadcast address.
Multicast	The number of good packets received during this sampling interval that were directed to a multicast address. This number does not include packets addressed to the broadcast address.
Utilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
CRC Align	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
Oversize	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
Fragments	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (AlignmentError). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Jabbers	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Dropped	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected.
Collisions	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

---

rmon alarm

Use the **rmon alarm** global configuration command to configure alarm conditions. To remove an alarm, use the **no** form of this command.

Syntax

rmon alarm *index variable interval rthreshold fthreshold revent fevent* [**type** *type*] [**startup** *direction*] [**owner** *name*]

no rmon alarm *index*

- *index*—The alarm index (Range: **1-65535**).
- *variable*—The variable object identifier to be sampled.
- *interval*—The interval in seconds over which the data is sampled and compared with the rising and falling thresholds (Range: **1-4294967295**).
- *rthreshold*—Rising Threshold (Range: **1-4294967295**).
- *fthreshold*—Falling Threshold (Range: **1-4294967295**).
- *revent*—The Event index used when a rising threshold is crossed (Range: **1-65535**).
- *fevent*—The Event index used when a falling threshold is crossed (Range: **1-65535**).
- **type** *type*—The sampling method for the selected variable and calculating the value to be compared against the thresholds. If the method is

absolute, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the method is **delta**, the selected variable value at the last sample is subtracted from the current value, and the difference compared with the thresholds.

- **startup** *direction*—The alarm that may be sent when this entry is first set to valid. If the first sample after this entry becomes valid is greater than or equal to the *rthreshold*, and *direction* is equal to **rising** or **rising-falling**, then a single rising alarm is generated. If the first sample after this entry becomes valid is less than or equal to the *fthreshold*, and *direction* is equal to **falling** or **rising-falling**, then a single falling alarm is generated.
- **owner** *name*—Enter a name that specifies who configured this alarm. If unspecified, the name is an empty string.

Default Configuration

The following parameters have the following default values:

- **type** *type*—If unspecified, the type is **absolute**.
- **startup** *direction*—If unspecified, the startup direction is **rising-falling**.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example configures the following alarm conditions:

- Alarm index—1
- Variable identifier—1.3.6.1.2.1.16.1.1.1.18.1
- Sample interval—10 seconds
- Rising Threshold—100
- Falling Threshold—20
- Rising threshold event index—10
- Falling threshold event index—20

```
console(config)# rmon alarm 1 1.3.6.1.2.1.16.1.1.1.18.1 10 100 20 10 20
```

---

show rmon alarm-table

Use the **show rmon alarm-table** privileged EXEC command to display the alarms summary table.

Syntax

show rmon alarm-table

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the alarms summary table.

```
Console# show rmon alarm-table

Index OID Owner
----- ---------------------- -------
1 1.3.6.1.2.1.2.2.1.10.1 CLI
2 1.3.6.1.2.1.2.2.1.10.1 Manager
3 1.3.6.1.2.1.2.2.1.10.9 CLI
```

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the entry.
OID	Monitored variable OID.
Owner	The entity that configured this entry.

---

show rmon alarm

Use the **show rmon alarm** privileged EXEC command to display alarm configuration.

Syntax

show rmon alarm *number*

- *number*—Alarm index (Range: **1-65535**).

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the RMON alarm 1 information.

```
Console# show rmon alarm 1

Alarm 1

-------

OID: 1.3.6.1.2.1.2.2.1.10.1

Last sample Value: 878128

Interval: 30

Sample Type: delta

Startup Alarm: rising

Rising Threshold: 8700000

Falling Threshold: 78
```

```
Rising Event: 1


Falling Event: 1


Owner: CLI
```

The following table describes the significant fields shown in the display:

Field	Description
OID	Monitored variable OID.
Last Sample Value	The statistic value during the last sampling period. For example, if the sample type is delta, this value is the difference between the samples at the beginning and end of the period. If the sample type is absolute, this value is the sampled value at the end of the period.
Alarm	Alarm index.
Owner	The entity that configured this entry.
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Sample Type	The method of sampling the variable and calculating the value compared against the thresholds. If the value is **absolute**, the value of the variable is compared directly with the thresholds at the end of the sampling interval. If the value is **delta**, the value of the variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
Startup Alarm	The alarm that may be sent when this entry is first set. If the first sample is greater than or equal to the Rising Threshold, and Startup Alarm is equal to rising or rising and falling, then a single rising alarm is generated. If the first sample is less than or equal to the Falling Threshold, and Startup Alarm is equal falling or Rising and Falling, then a single falling alarm is generated.
Rising Threshold	A sampled statistic threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.
Falling Threshold	A sampled statistic threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.
Rising Event	The Event index used when a rising threshold is crossed.
Falling Event	The Event index used when a falling threshold is crossed.

---

rmon event

Use the **rmon event** global configuration command to configure an event. To remove an event, use the **no** form of this command.

Syntax

rmon event *index type* [**community** *text*] [**description** *text*] [**owner** *name*]

no rmon event *index*

- *index*—The event index (Range: **1-65535**).
- *type*—The notification type that the device generates about this event. Can have the following values: **none**, **log**, **trap**, **log-trap**. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
- **community** *text*—If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.
- **description** *text*—A comment describing this event.
- **owner** *name*—Enter a name that specifies who configured this event. If unspecified, the name is an empty string.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example configures an event with the trap index of 10.

```
Console (config)# rmon event 10 log community delta
```

---

show rmon events

Use the **show rmon events** privileged EXEC command to display the RMON event table.

Syntax

show rmon events

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example describes RMON events.

```
Console# show rmon events


Index Description Type Community Owner Last time sent


----- ----------- ---------- ---------- -------- ------------------


1 Errors Log CLI Jan 18 2002 23:58:17


2 High Broadcast Log-Trap device Manager Jan 18 2002 23:59:48
```

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the event.
Description	A comment describing this event.
Type	The type of notification that the device generates about this event. Can have the following values: **none**, **log**, **trap**, **log-trap**. In the case of **log**, an entry is made in the log table for each event. In the case of **trap**, an SNMP trap is sent to one or more management stations.
Community	If an SNMP trap is sent, it is sent to the SNMP community specified by this octet string.
Owner	The entity that configured this event.
Last time sent	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

---

show rmon log

Use the **show rmon log** privileged EXEC command to display the RMON logging table.

Syntax

show rmon log [*event*]

- *event*—Event index (Range: **0-65535**).

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the RMON logging table.

```
Console# show rmon log

Maximum table size: 500

Event Description Time

----- ----------- --------------------

1 Errors Jan 18 2002 23:48:19

1 Errors Jan 18 2002 23:58:17

2 High Broadcast Jan 18 2002 23:59:48

Console# show rmon log

Maximum table size: 500 (800 after reset)

Event Description Time

----- ----------- --------------------

1 Errors Jan 18 2002 23:48:19

1 Errors Jan 18 2002 23:58:17

2 High Broadcast Jan 18 2002 23:59:48
```

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the event.
Description	A comment describing this event.
Time	The time this entry created.

---

rmon table-size

Use the **rmon table-size** global configuration command to configure the maximum RMON tables sizes. To return to the default configuration, use the **no** form of this command.

Syntax

rmon table-size {**history** *entries* | **log** *entries*}

no rmon table-size {**history** | **log**}

- **history** *entries*—Maximum number of history table entries (Range: **20-32767**).
- **log** *entries*—Maximum number of log table entries (Range: **20-32767**).

Default Configuration

History table size is **270**.

Log table size is **100**.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example configures the maximum RMON history table sizes to 1000 entries.

```
Console (config)# rmon table-size history 1000
```

Back to Contents Page

Back to Contents Page

SNMP Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- snmp-server community
- snmp-server contact
- snmp-server location
- snmp-server enable traps
- snmp-server trap authentication
- snmp-server host
- snmp-server set
- show snmp

---

snmp-server community

Use the **snmp-server community** global configuration command to set up the community access string to permit access to the SNMP protocol. To remove the specified community string, use the **no** form of this command.

Syntax

snmp-server community *string* [**ro** | **rw** | **su**] [*ip-address*]

no snmp-server community *string* [*ip-address*]

- *string*—Character string, up to 20 characters, that acts like a password and permits access to the SNMP protocol.
- **ro**—Specifies read-only access.
- **rw**—Specifies read-write access.
- **su**—Specifies SNMP administrator access.
- *ip-address*—Management station IP address.

Default Configuration

The default is read-only and if no IP address is entered, all IP addresses are allowed.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example sets up the community access string `public` to permit administrative access to the SNMP protocol, at an administrative station with the IP address `192.168.1.20`.

```
```

```
Console (config)# snmp-server community public su 192.168.1.20
```

---

snmp-server contact

Use the **snmp-server contact** global configuration command to set up a system contact. To remove the system contact information, use the **no** form of the command.

Syntax

snmp-server contact *text*

no snmp-server contact

- *text*—Character string, up to 160 characters, describing the system contact information.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example sets up Dell_Technical_Support as the system contact point.

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

---

snmp-server location

Use the **snmp-server location** global configuration command to set up information about where the device is located. To remove the location string, use the **no** form of this command.

Syntax

snmp-server location *text*

no snmp-server location

- *text*—Character string, up to 160 characters, describing the system location.

Default Configuration

The default is no community.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example sets the device location as New_York.

```
Console (config)# snmp-server location New_York
```

---

snmp-server enable traps

Use the **snmp-server enable traps** global configuration command to enable the switch to send SNMP traps. To disable SNMP traps, use the **no** form of the command.

Syntax

snmp-server enable traps

no snmp-server enable traps

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the command to enable SNMP traps.

```
Console (config)# snmp-server enable traps
```

---

snmp-server trap authentication

Use the **snmp-server trap authentication** global configuration command to enable the switch to send Simple Network Management Protocol traps when authentication failed. To disable SNMP authentication failed traps, use the **no** form of this command.

Syntax

snmp-server trap authentication

no snmp-server trap authentication

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example enables authentication when SNMP traps failed.

```
```

```
Console (config)# snmp-server trap authentication
```

---

snmp-server host

Use the **snmp-server host** global configuration command to specify the recipient of Simple Network Management Protocol (SNMP) notification operation. To remove the specified host, use the **no** form of this command.

Syntax

snmp-server host *host-addr community-string* [**1** | **2**]

no snmp-server host *host-addr*

- *host-addr*—The host (the targeted recipient) internet address.
- *community-string*—Password-like community string, up to 20 characters, sent with the notification operation.
- **1**—SNMPv1 traps is used.
- **2**—SNMPv2 traps is used (Default).

Default Configuration

The default version for traps is **SNMPv2**.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example enables SNMP traps for host `10.1.1.1` with community string `management` using SNMPv2.

```
Console (config)# snmp-server host 10.1.1.1 management 2
```

---

snmp-server set

Use the **snmp-server set** global configuration command to set the SNMP MIB value by the CLI.

Syntax

snmp-server set *variable name* [*name value* ...]

- *variable name*—The name of the MIB variable name to be modified.
- *name value*—List of name and value pairs. In case of scalar MIBs there is only a single pair of name values. In case of entry in a table the first pairs are the indexes, followed by one or more fields.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

Although the CLI can set any required configuration, there might be a situation where an SNMP user sets a MIB variable that doesn't have an equivalent command. Use the **snmp-server set** command for those situations.

Examples

The following example sets the scalar MIB sysName to the value dell.

```
Console (config)# snmp-server set sysName sysName dell
```

The following example sets the entry MIB rndCommunityTable with keys 0.0.0.0 and public. The field rndCommunityAccess gets the value super and the rest of the fields get their default values.

```
Console (config)# snmp-server set rndCommunityTable rndCommunityMngStationAddr 0.0.0.0 rndCommunityString public rndCommunityAccess super
```

---

show snmp

Use the **show snmp** privileged EXEC command to display the SNMP status.

Syntax

show snmp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays SNMP communication status.

```
Console# show snmp


Community-String Community-Access IP address

---------------- ---------------- -----------

public read only All

private read write 172.16.1.1

private read write 172.17.1.1



Traps are enabled.

Authentication trap is enabled.



Trap-Rec-Address Trap-Rec-Community Version

---------------- ------------------ --------

192.122.173.42 public 2
```

```
System Contact: Robert


System Location: Marketing
```

Back to Contents Page

Back to Contents Page

Spanning Tree Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- spanning-tree
- spanning-tree mode
- spanning-tree forward-time
- spanning-tree hello-time
- spanning-tree max-age
- spanning-tree priority
- spanning-tree disable
- spanning-tree cost
- spanning-tree port-priority
- spanning-tree portfast
- clear spanning-tree detected-protocols
- spanning-tree link-type
- show spanning-tree

---

spanning-tree

Use the **spanning-tree** global configuration command to enable spanning tree functionality. To disable spanning tree functionality, use the **no** form of this command.

Syntax

spanning-tree

no spanning-tree

Default Configuration

Spanning tree is enabled.

Command Modes

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables spanning tree functionality.

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

---

spanning-tree mode

Use the **spanning-tree mode** global configuration command to configure the spanning tree protocol currently running. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree mode {**stp** | **rstp**}

no spanning-tree mode

- **stp**—RSTP is not supported
- **rstp**—RSTP is supported

Default Configuration

spanning tree protocol is supported (stp).

Command Modes

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the spanning tree protocol to RSTP.

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

---

spanning-tree forward-time

Use the **spanning-tree forward-time** global configuration command to configure the spanning tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state.

To reset the default forward time, use the **no** form of this command.

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

- *seconds*—Time in seconds (Range: **4-30**).

Default Configuration

The default forwarding-time for IEEE Spanning Tree Protocol (STP) is **15** seconds.

Command Modes

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures spanning tree bridge forward time.

```
Console(config)# spanning-tree forward-time 25
```

---

spanning-tree hello-time

Use the **spanning-tree hello-time** global configuration command to configure the spanning tree bridge hello time, which is how often the switch broadcasts hello messages to other switches only if it is the root bridge. To reset the default hello time, use the **no** form of this command.

Syntax

spanning-tree hello-time *seconds*

no spanning-tree hello-time

- *seconds*—Time in seconds (Range: **1-10**).

Default Configuration

The default hello time for IEEE Spanning Tree Protocol (STP) is **2** seconds.

Command Modes

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures spanning tree bridge hello time.

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

---

spanning-tree max-age

Use the **spanning-tree max-age** global configuration command to configure the spanning tree bridge maximum age. To reset the default maximum age, use the **no** form of this command.

Syntax

spanning-tree max-age *seconds*

no spanning-tree max-age

- *seconds* -Time in seconds (Range: **6-40**).

Default Configuration

The default max-age for IEEE STP is **20** seconds.

Command Modes

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the spanning tree bridge maximum-age.

```
Console(config)# spanning-tree max-age 10
```

---

spanning-tree priority

Use the **spanning-tree priority** global configuration command to configure the spanning tree priority. The priority value is used to determine which bridge is elected as the root bridge. To reset the default spanning tree priority, use the **no** form of this command.

Syntax

spanning-tree priority *priority*

no spanning-tree priority

- *priority*—Priority of the bridge (Range: **0-61440** in steps of 4096).

Default Configuration

The default STP bridge priority according to IEEE 802.10 is **32768**.

Command Modes

Global Configuration Mode

User Guidelines

The lower the priority, the more likely the bridge is to be elected as the root bridge.

Example

The following example configures spanning tree priority.

```
Console(config)# spanning-tree priority 12288
```

---

spanning-tree disable

Use the **spanning-tree disable** interface configuration command to disable spanning tree on a specific port. To enable spanning tree on a port, use the **no** form of this command.

Syntax

spanning-tree disable

no spanning-tree disable

Default Configuration

By default, all ports are enabled for spanning tree.

Command Modes

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example disables the spanning tree on port 1/e5.

```
Console(config)# interface ethernet 1/e5

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

---

spanning-tree cost

Use the **spanning-tree cost** interface configuration command to configure the spanning tree path cost for a port. To reset the default port path cost, use the **no** form of this command.

Syntax

spanning-tree cost *cost*

no spanning-tree cost

- *cost*—The port path cost (Range: **1-65535**).

Default Configuration

The default costs are as follows:

- **Port-channel—4**
- **1 Giga—4**
- **100M—19**
- **10M—100**

Command Modes

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures spanning tree cost on port 1/e5 to 35000.

```
Console(config)# interface ethernet 1/e5

Console(config-if)# spanning-tree cost 35000
```

---

spanning-tree port-priority

Use the **spanning-tree port-priority** interface configuration command to configure port priority. To reset the default port priority, use the **no** form of this command.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

- *priority*—The port priority (Range: **0-240** in steps of 16).

Default Configuration

The default port-priority for IEEE 802.10 (STP) is **128**.

Command Modes

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures spanning priority on port 1/e5 to 96.

```
Console(config)# interface ethernet 1/e5

Console(config-if)# spanning-tree port-priority 96
```

---

spanning-tree portfast

Use the **spanning-tree portfast** interface configuration command to enable PortFast Mode. In PortFast Mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the timer to expire. To disable PortFast Mode, use the **no** form of this command. This command when in **rstp** mode sets port to an edgeport.

Syntax

spanning-tree portfast

no spanning-tree portfast

Default Configuration

PortFast Mode is disabled.

Command Modes

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

This feature should be used only with interfaces connected to end stations. Otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operations.

Example

The following example enables PortFast Mode on port 1/e5.

```
Console(config)# interface ethernet 1/e5

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

---

clear spanning-tree detected-protocols

Use the **clear spanning-tree detected-protocols** privileged EXEC command to restart the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.

Syntax

clear spanning-tree detected-protocols [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—An ethernet port. The full syntax is: *unit/port*.
- *port-channel-number*—A port-channel index.

Default Configuration

If no interface is specified, the action is applied to all interfaces.

Command Modes

Privileged EXEC Mode

User Guidelines

This feature should be used only when working in RSTP mode. It is used to force the port to test if it can migrate to RSTP.

Example

The following example restarts the protocol migration process (forces the renegotiation with neighboring switches) on port 1/e3.

```
Console# clear spanning-tree detected-protocols ethernet 1/e3
```

---

spanning-tree link-type

Use the **spanning-tree link-type** interface configuration command to override the default link-type setting. To reset the default, use the **no** form of this

command.

Syntax

spanning-tree link-type {**point-to-point** | **shared**}

no spanning-tree spanning-tree link-type

- **point-to-point**—Specify the port link type as point-to-point.
- **shared**—Specify that the port link type is shared.

Default Configuration

The switch derives the link type of a port from the duplex mode. A full-duplex port is considered a point-to-point link, and a half-duplex port is considered a shared link.

Command Modes

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example forces shared link-type on port 1/e5.

```
Console(config)# interface ethernet 1/e5

Console(config-if)# spanning-tree link-type shared
```

---

show spanning-tree

Use the **show spanning-tree** privileged EXEC command to display spanning tree configuration.

Syntax

show spanning-tree [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—An ethernet port. The full syntax is: *unit/port*.
- *port-channel-number*—A port-channel index.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays spanning tree information.

```
Console# show spanning-tree

Spanning tree enabled mode RSTP

Root ID Priority 32768

Address 0001.4297.e000

Cost 57

Port 1/e1

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769

Address 0002.4b29.7a00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Number of topology changes 2 last change occurred 2d18h ago

Times: hold 1, topology change 35, notification 2
```

```
hello 2, max age 20, forward delay 15

Interface Port ID Designated Port ID

Name Prio.Nbr Sts Cost Cost Bridge ID Prio.Nbr

---------- -------- ---- --- ---------------------- --------

1/e1 128.1 FWD 19 38 32768 0030.9441.62c1 128.25

1/e2 128.2 FWD 19 57 32769 0002.4b29.7a00 128.2

ch1 128.65 FWD 19 57 32769 0002.4b29.7a00 128.65
```

The following example displays spanning tree information for port 1/e1.

```
Console# show spanning-tree ethernet 1/e1

Interface Port ID Designated Port ID

Name Prio.Nbr Cost Sts Cost Bridge ID Prio.Nbr

---------- -------- ---- --- ---------------------- --------

1/e1 128.1 19 FWD 38 32768 0030.9441.62c1 128.25



Spanning tree enabled

Type: point-to-point (configured: auto)

Port Fast: no (configured: no)

Number of transitions to forwarding state: 1

BPDU: sent 2, received 120638
```

Back to Contents Page

Back to Contents Page

SSH Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- ip ssh port
- ip ssh server
- crypto key generate dsa
- crypto key generate rsa
- ip ssh pubkey-auth
- crypto key pubkey-chain ssh
- user-key
- key-string
- show ip ssh
- show crypto key mypubkey
- show crypto key pubkey-chain ssh

---

ip ssh port

Use the **ip http port** global configuration command to specify the TCP port to be used by the SSH server. To use the default port, use the **no** form of this command.

Syntax

ip ssh port *port-number*

no ip ssh port

- *port-number*—Port number for use by the SSH server (Range: **0-65535**).

Default Configuration

The default value is **22**.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example specifies the port to be used by the SSH server.

```
Console (config)# ip ssh port 8080
```

---

ip ssh server

Use the **ip ssh server** global configuration command to enable the device to be configured from SSH. To disable this function use the **no** form of this command.

Syntax

ip ssh server

no ip ssh server

Default Configuration

This default is enabled to be configured from SSH.

Command Mode

Global Configuration Mode

User Guidelines

If encryption keys are not generated, the SSH server is in standby until the keys are generated. To generate SSH server keys, use the commands crypto key generate rsa, and crypto key generate dsa.

Examples

The following example enables the device to be configured from a SSH server.

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

---

crypto key generate dsa

Use the **ip ssh server** global configuration command to generate DSA key pairs.

Syntax

crypto key generate dsa

Default Configuration

DSA key pairs do not exist.

Command Mode

Global Configuration Mode

User Guidelines

DSA keys are generated in pairs, one public DSA key and one private DSA key. If the device already has DSA keys, a warning and prompt to replace the existing keys with new keys is displayed.

This command is not saved in the startup configuration, however, the keys generated by this command are saved in the running configuration (which is never displayed to the user or backed up to another device).

Examples

The following example generates DSA key pairs.

```
Console (config)# crypto key generate dsa

This may take several minutes depending on the length.

Console (config)#
```

---

crypto key generate rsa

Use the **crypto key generate rsa** global configuration command to generate RSA key pairs.

Syntax

crypto key generate rsa

Default Configuration

RSA key pairs do not exist.

Command Mode

Global Configuration Mode

User Guidelines

DSA keys are generated in pairs, one public DSA key and one private DSA key. If the device already has DSA keys, a warning and prompt to replace the existing keys with new keys is displayed.

This command is not saved in the startup configuration, however, the keys generated by this command are saved in the running configuration (which is never displayed to the user or backed up to another device).

Examples

The following example generates RSA key pairs.

```
Console (config)# crypto key generate rsa

This may take several minutes depending on the length.

Console (config)#
```

---

ip ssh pubkey-auth

Use the **ip ssh pubkey-auth** global configuration command to enable public key authentication for incoming SSH sessions. To disable this function, use the **no** form of this command.

Syntax

ip ssh pubkey-auth

no ip ssh pubkey-auth

Default Configuration

The function is disabled.

Command Mode

Global Configuration Mode

User Guidelines

AAA authentication is independent.

Examples

The following example enables public key authentication for incoming SSH sessions.

```
Console (config)# ip ssh pubkey-auth
```

---

crypto key pubkey-chain ssh

Use the **crypto key pubkey-chain ssh** global configuration command to enter SSH Public Key-Chain Configuration Mode. The mode is used to manually specify other device public keys such as SSH client public keys.

Syntax

crypto key pubkey-chain ssh

Default Configuration

By default there are no keys.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example enters the SSH Public Key-Chain Configuration Mode.

```
Console(config)# crypto key pubkey-chain ssh

Console(config-pubkey-chain)#
```

---

user-key

Use the **user-key** SSH public key-chain configuration command to specify which SSH public key is manually configured and enters the SSH public key-string

configuration command. To remove a SSH public key, use the **no** form of this command.

Syntax

user-key *username*

no user-key *username*

- *username*—Specifies the remote SSH client username.

Default Configuration

By default there are no keys.

Command Mode

SSH Public Key-Chain Configuration Mode

User Guidelines

Follow this command with the key-string command to specify the key.

Examples

The following example enables a SSH public key to be manually configured for the SSH public-key chain.

```
Console(config)# crypto key pubkey-chain ssh

Console(config-pubkey-chain)# user-key bob

Console(config-pubkey-key)#
```

---

key-string

Use the **key-string** SSH public key-string configuration command to manually specify a SSH public key.

Syntax

key-string {**rsa** | **dss**}

- **rsa**—RSA key
- **dss**—DSS key

Default Configuration

By default the keys do not exist.

Command Mode

SSH Public Key-string configuration

User Guidelines

Use this command to specify which SSH public key to manually configure next.

UU-encoded DER format is the same format in authorized_keys file used by OpenSSH.

To complete the command, enter the row with no characters.

Examples

The following example enters public key strings for SSH public key clients.

```
Console(config)# crypto key pubkey-chain ssh

Console(config-pubkey-chain)# user-key bob

Console(config-pubkey-key)# key-string rsa

AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl

Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+

ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+

Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g

kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq

muSn/Wd05iDX2IExQWu08licglk02LYciz

+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
```

```
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA

6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+

Rmt5nhhqdAtN/4oJfce166DqVX1gWmN

zNR4DYDvSzg0lDnwCAC8Qh

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

---

show ip ssh

Use the **show ip ssh** privileged EXEC command to display the SSH server configuration.

Syntax

show ip ssh

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the SSH server configuration.

```
Console# show ip ssh

SSH server enabled. Port: 22
```

```
RSA key was generated.

DSA key was generated.

SSH Public Key Authentication is enabled.

Active incoming sessions:

IP address SSH username Version Cipher Auth Code

---------- ------------ ------- ------ ---------

172.16.0.1 John Brown 1.5 3DES HMAC-SH1
```

---

show crypto key mypubkey

Use the **show crypto key mypubkey** privileged EXEC command to display the SSH public keys on the device.

Syntax

show crypto key mypubkey [**rsa** | **dsa**]

- **rsa**—RSA key
- **dsa**—DSA key

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the SSH public keys on the device.

```
Console# show crypto key mypubkey rsa

RSA key data:

005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22

04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2

BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 87685768

Fingerprint(Hex): 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86

Fingerprint(Bubble Babble): yteriuwt jgkljhglk yewiury hdskjfryt gfhkjglk
```

---

show crypto key pubkey-chain ssh

Use the **show crypto key pubkey-chain ssh** privileged EXEC command to display SSH public keys stored on the device.

Syntax

show crypto key pubkey-chain ssh [**username** *username*] [**fingerprint bubble-babble** | **hex**]

- *username*—Specifies the remote SSH client username.
- **bubble-babble**—Fingerprints in Bubble Babble format.
- **hex**—Fingerprint in Hex format. If fingerprint is unspecified it defaults to Hex format.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays all SSH public keys stored on the device.

```
Console# show crypto key pubkey-chain ssh

Username Fingerprint

-------- -----------------------------------------------

bob 9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86

john 98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:87:C8
```

The following example displays the SSH public key called bob.

```
Console# show crypto key pubkey-chain ssh bob

Username: bob

Key: 005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22 04AEF1BA A54028A6 9ACC01C5 129D99E4

Fingerprint: 9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
```

Back to Contents Page

Back to Contents Page

Syslog Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- logging on
- logging
- logging console
- logging buffered
- logging buffered size
- clear logging
- logging file
- clear logging file
- show logging
- show logging file
- show syslog-servers

---

logging on

Use the **logging on** global configuration command to control error message logging. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously with respect to the process that generated the messages. To disable the logging process, use the **no** form of this command.

Syntax

logging on

no logging on

Default Configuration

Logging is enabled.

Command Mode

Global Configuration Mode

User Guidelines

The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or syslog server. Logging on and off for these destinations can be individually configured using the **logging buffered**, **logging file**, and **logging** global configuration commands. However, if the **logging on** command is disabled, no messages are sent to these destinations. Only the console receives messages.

Examples

The following example enables logging.

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

---

logging

Use the **logging** global configuration command to log messages to a syslog server. To delete the syslog server with the specified address from the list of syslogs, use the **no** form of this command.

Syntax

logging *ip-address* [**port** *port*] [**severity** *level*] [**facility** *facility*] [**description** *text*]

no logging *ip-address*

- *ip-address*—Host IP address used as a syslog server.
- *port*—Port number for syslog messages. If unspecified, the port number defaults to **514** (Range: **1-65535**).
- *level*—Limits the logging of messages to the syslog servers to a specified level: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, notifications, **informational** and **debugging**. If unspecified, the level is **errors**.
- *facility*—The facility that is indicated in the message. Can be one of the following values: **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local 6**, **local7**, and **no-maps**. If unspecified, the port number defaults to **local7**.
- *text*—Syslog server description.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

Multiple syslog servers can be used.

If no specific severity level is specified, the global values apply to each server.

When the device is rebooted, the log is kept, even when logging is disabled.

Examples

The following example logs messages with a severity level `critical` to a syslog server with an IP address `10.1.1.1`.

```
Console (config)# logging 10.1.1.1 severity critical
```

---

logging console

Use the **logging console** global configuration command to limit messages logged to the console based on severity. To disable logging to the console terminal, use the **no** form of this command.

Syntax

logging console *level*

no logging console

- *level*—Limits the logging of messages displayed on the console to a specified level: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, **debugging**.

Default Configuration

The default is **informational**.

Command Mode

Global Configuration Mode

User Guidelines

All severities below the selected severity level are automatically selected.

Examples

The following example limits messages logged to the console to be based on the `errors` severity level.

```
Console (config)# logging console errors
```

---

logging buffered

Use the **logging buffered** global configuration command to limit syslog messages displayed from an internal buffer based on severity. To cancel buffer use, use the **no** form of this command.

Syntax

logging buffered *level*

no logging buffered

- *level*—Limits the message logging to a specified level buffer: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, **debugging**.

Default Configuration

The default level is **informational**.

Command Mode

Global Configuration Mode

User Guidelines

All the syslog messages are logged to the internal buffer. This command limits the commands displayed to the user.

Examples

The following example limits syslog messages displayed from an internal buffer based on the debugging severity level.

```
Console (config)# logging buffered debugging
```

---

logging buffered size

Use the **logging buffered size** global configuration command to set the number of syslog messages stored in the internal buffer. To return the number of messages stored in the internal buffer to the default value, use the **no** form of this command.

Syntax

logging buffered size *number*

no logging buffered size

- *number*—Numeric value indicating the maximum number of messages stored in the history table (Range: **1-400**).

Default Configuration

The default number of messages is **200**.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example changes the number of syslog messages stored in the internal buffer to 300.

```
Console (config)# logging buffered size 300
```

---

clear logging

Use the **clear logging** privileged EXEC command to clear messages from the internal logging buffer.

Syntax

clear logging

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example clears messages from the internal syslog message logging buffer.

```
Console# clear logging

Clear logging buffer [y/n]
```

```
Console#
```

---

logging file

Use the **logging file** global configuration command to limit syslog messages sent to the logging file based on severity. To cancel the buffer, use the **no** form of this command.

Syntax

logging file *level*

no logging file

- *level*—Limits message logging to the buffer for a specified level, which includes one of the following: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational** and **debugging.**

Default Configuration

The default severity level is **errors**.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example limits syslog messages sent to the logging file based on the `alerts` severity level.

```
Console (config)# logging file alerts
```

---

clear logging file

Use the **clear logging file** privileged EXEC command to clear messages from the logging file.

Syntax

clear logging file

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example clears messages from the logging file.

```
Console# clear logging file

Clear logging file [y/n]

Erasing file syslog1.....done

Console#
```

---

show logging

Use the **show logging** privileged EXEC command to display logging information and syslog messages stored in the internal logging buffer.

Syntax

show logging

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays logging information about the syslog messages stored in the internal logging buffer.

```
Console # show logging

Console logging: level debugging. Console Messages: 0 Dropped (severity).

Buffer logging: level debugging. Buffer Messages: 11 Logged, 200 Max.

File logging: level notifications. File Messages: 0 Dropped (severity).

Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped (severity).

Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped (severity).

2 messages were not logged (resources)

Buffer log:

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e0, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e1, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e2, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e3, changed state to up

11-Aug-2002 15:41:43: %SYS-5-CONFIG_I: Configured from memory by console

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

```
11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e0, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e1, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e2, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e3, changed state to down
```

---

show logging file

Use the **show logging file** privileged EXEC command to display the state of logging and the syslog messages stored in the logging file.

Syntax

show logging file

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the state of logging and the syslog messages stored in the logging file.

```
Console # show logging file

Console logging: level debugging. Console Messages: 0 Dropped (severity).

Buffer logging: level debugging. Buffer Messages: 11 Logged, 200 Max.

File logging: level notifications. File Messages: 0 Dropped (severity).
```

```
Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped (severity).

Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped (severity).

2 messages were not logged (resources)

File log:

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e0, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e1, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e2, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e3, changed state to up

11-Aug-2002 15:41:43: %SYS-5-CONFIG_I: Configured from memory by console

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e0, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e1, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e2, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e3, changed state to down
```

---

show syslog-servers

Use the **show syslog-servers** privileged EXEC command to display the syslog servers settings.

Syntax

show syslog-servers

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the syslog server settings.

```
Console# show syslog-servers

IP address Port Severity facility Description

---------- ---- -------- -------- -----------

192.180.2.27 514 Informational local7

192.180.2.28 514 Warning local7
```

Back to Contents Page

Back to Contents Page

System Management

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- ping
- reload
- clock set
- hostname
- asset-tag
- stack order
- show users
- show clock
- show system
- show version
- show system id

---

ping

Use the **ping user EXEC command** to send ICMP echo request packets to another node on the network.

Syntax

ping *host* [**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*]

- *host*—IP address being contacted.
- *packet_size*—Number of bytes in a packet, from 56 to 1472 bytes. The actual packet size is eight bytes larger than the size specified because the switch adds header information.
- *packet_count*—Number of packets to send, from 1 to 65535 packets. If 0 is entered it pings until stopped.
- *time_out*—Timeout in milliseconds to wait for each reply, from 1 to 65535 milliseconds.

Default Configuration

The default packet size is **56** bytes.

The default packet count is **4** packets.

The default time-out is **1000** milliseconds.

Command Mode

User EXEC Mode

User Guidelines

Press ESC to stop pinging. Following are sample results of the **ping** command:

- `Destination does not respond`—If the host does not respond, *no answer from host* appears in ten seconds.
- `Destination unreachable`—The gateway for this destination indicates that the destination is unreachable.
- `Network or host unreachable`—The switch found no corresponding entry in the route table.

Examples

The following example displays a ping to IP address 10.1.1.1.

```
Console> ping 10.1.1.1

64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms

64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms

64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms

64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms

64 bytes from 10.1.1.1: icmp_seq=4. time=11 ms

64 bytes from 10.1.1.1: icmp_seq=5. time=7 ms

64 bytes from 10.1.1.1: icmp_seq=6. time=7 ms

^C

----10.1.1.1 PING Statistics----

7 packets transmitted, 7 packets received, 0% packet loss

round-trip (ms) min/avg/max = 7/8/11

Console>
```

---

reload

Use the **reload** user EXEC command to reload the operating system.

Syntax

reload

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the prompt when entering the **reload** command.

```
Console >reload

This command will reset the whole system and disconnect your telnet session.

Do you want to continue (y/n) [n]?
```

---

clock set

Use the **clock set** user EXEC command to manually set the system clock.

Syntax

clock set *hh:mm:ss day month year*

or

clock set *hh:mm:ss month day year*

- *hh:mm:ss*—Current time in hours (military format), minutes, and seconds (0-23, mm: 0-59, ss: 0-59).
- *day*—Current day (by date) in the month (1-31).
- *month*—Current month using the first three letters by name (Jan, ... Dec).
- *year*—Current year (1998-2097).

Default Configuration

This command has no default configuration.

Command Mode

User EXEC Mode

User Guidelines

This device clock is not a Real Time Clock (RTC). When the device is rebooted or restarted, the clock setting is deleted.

Examples

The following example sets the system time.

```
Console> clock set 13:32:00 7 Mar 2002
```

---

hostname

Use the **hostname** global configuration command to specify or modify the device host name. To restore the default host name, use the **no** form of the command.

Syntax

hostname *name*

no hostname

- *name*—The name of this host.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example specifies dell as the device host name.

```
Console (config)# hostname dell
```

---

asset-tag

Use the **asset-tag** global configuration command to specify the device asset-tag. Use the **no** form of this command to restore the default host name.

Syntax

asset-tag [**unit** *unit*] *tag*

no asset-tag [**unit** *unit*]

- **unit** *unit*—Unit number. If unspecified defaults to the master unit number.
- *tag*—The device asset-tag.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example specifies the device asset tag.

```
Console (config)# asset-tag 45456
```

---

stack order

Use the **stack order** global configuration command to configure the unit physical order in the stack. To return to the default value, use the **no** form of this command.

Syntax

stack order *order1 order2* {*order3* ...}

no stack order

- *order1 order2* {*order3* ...}—Unit order. All the units in the stack are configured in the same command.

Default Configuration

The default value is the unit number.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example configures the device 2 as the first unit and device 1 as the second unit in the stack.

```
Console (config)# stack order 2 1
```

---

show users

Use the **show users** user EXEC command to display information about the active users.

Syntax

show users

Default Configuration

This command has no default configuration.

Command Mode

User EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays information about the active users.

```
Console> show users


Username Idle Time Remote IP Protocol


---------- --------- --------- ---------


Bob 00:00:00 Serial


Betty 00:08:19 172.16.0.1 Telnet


Robert - 172.16.0.8 HTTP
```

---

show clock

Use the **show clock** user EXEC command to display the time and date from the system clock.

Syntax

show clock

Default Configuration

This command has no default configuration.

Command Mode

User EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the time and date from the system clock.

```
Console> show clock


15:29:03 Jun 17 2002
```

---

show system

Use the **show system** user EXEC command to display system information.

Syntax

show system [**unit** *unit*]

- **unit** *unit*—Unit number. If unspecified, defaults to the master unit number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the system information.

```
Console> show system

System Description: Corporate

System Up Time (days,hour:min:sec): 1,22:38:21

System Contact:

System Name: Console 1

System location:

power supply status : OK

MAC Address: xxxx.xxxx.xxxx

Sys Object ID:
```

---

show version

Use the **show version** user EXEC command to display the system version information.

Syntax

show version [**unit** *unit*]

- **unit** *unit*—Unit number. If unspecified defaults to the master unit number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays a system version (this version number is only for demonstration purposes).

```
Console> show version

SW version x.xxx (date xx-xxx-xxxx time 17:34:19)

Boot version x.xxx (date xx-xxx-xxxx time 11:48:21)

HW version x.x.x

Unit SW version Boot version HW version

----- ---------- ------------ ------------

1 3.131 2.178 1.0.0

2 3.131 2.178 1.0.0
```

---

show system id

Use the **show system id** user EXEC command to display the system identification information.

Syntax

show system id [**unit** *unit*]

- **unit** *unit*—Unit number. If unspecified, defaults to the master unit number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC Mode

User Guidelines

The tag information is on a device by device basis.

Examples

The following example displays the system identification information.

```
Console> show system id

Service Tag: 89788978

Serial number: 8936589782

Asset tag: 7843678957
```

Back to Contents Page

Back to Contents Page

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

NOTE: A NOTE indicates important information that helps you make better use of your computer.

NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

CAUTION: A CAUTION indicates a potential for property damage, personal injury, or death.

April 2003 P/N J0926 Rev. A00

Back to Contents Page

Back to Contents Page

User Interface Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- enable
- disable
- login
- exit(configuration)
- exit(EXEC)
- end
- help
- history
- history size
- debug-mode
- show history
- show privilege

---

enable

Use the **enable** user EXEC command to enter the Privileged EXEC Mode.

Syntax

enable [*privilege-level*]

- *privilege-level*—Privilege level required to enter the system (Range: **1-15**).

Default Configuration

The default privilege level is **15**.

Command Mode

User EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example shows how to enter privileged mode:

```
Console> enable

enter password:

Console#
```

disable

Use the **disable** privileged EXEC command to return the prompt to User EXEC Mode.

Syntax

disable [*privilege-level*]

- *privilege-level*—Privilege level required to enter the system (Range: **1-15**).

Default Configuration

The default privilege level is **1**.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example shows how to return to User EXEC Mode.

```
Console# disable


Console>
```

login

Use the **login** privileged EXEC command to exit the EXEC mode and log on again.

Syntax

login

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays how to exit the EXEC mode and log on again.

```
Console > enable

Console#

Console# login

Console>
```

---

exit(configuration)

Use the **exit** command to exit any configuration mode and enter the next highest mode in the CLI mode hierarchy.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

All command modes

User Guidelines

There are no user guidelines for this command.

Examples

The following example changes the configuration mode from Interface Configuration Mode to User EXEC Mode.

```
Console(config-if)# exit

Console(config)# exit

Console#
```

---

exit(EXEC)

Use the **exit** user EXEC command to close an active terminal session by logging off the device.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

User EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example closes an active terminal session.

```
Console> exit
```

---

end

The **end** global configuration mode command returns the command mode to Privileged Mode.

Syntax

end

Default Configuration

This command has no default configuration.

Command Mode

All command modes

User Guidelines

There are no user guidelines for this command.

Examples

The following example returns the command mode to Privileged Mode.

```
Console (config-if)# end

Console #
```

---

help

Use the **help** command to display a brief description of the help system.

Syntax

help

Default Configuration

This command has no default configuration.

Command Mode

All command modes

User Guidelines

There are no user guidelines for this command.

---

history

Use the **history** line configuration command to enable the command history function. To disable the command history feature, use the **no** form of this command.

Syntax

history

no history

Default Configuration

The history function is enabled.

Command Mode

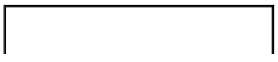
Line Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example enables the command history function.



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

---

history size

Use the **history size** line configuration command to set the command history buffer size for a particular line. To reset the command history buffer size to the default, use the **no** form of this command.

Syntax

history size *number-of-commands*

no history size

- *number-of-commands*—Number of commands that the system records in its history buffer (Range: **0-256**).

Default Configuration

The default history buffer size is **10**.

Command Mode

Line Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example changes the command history buffer size to **100** entries for a particular line.

```
Console (config-line)# history size 100
```

---

debug-mode

The **debug-mode** privilege EXEC command switches the mode to debug.

Syntax

debug-mode

Default Configuration

This command has no default configuration.

Command Mode

Privilege EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example enables the debug command interface.

```
console# debug

>debug

Enter DEBUG Password: *****

DEBUG>
```

---

show history

Use the **show history** privileged EXEC command to list the commands entered in the current session.

Syntax

show history

Default Configuration

This command has no default configuration.

Command Mode

Privilege EXEC Mode

User Guidelines

The command in the buffer also includes commands that were not executed.

The commands are listed from the first to the latest command.

The buffer remains unchanged when entering the configuration mode and returning back.

Examples

The following example displays the all commands entered while in the current Privileged EXEC Mode.

```
Console# show history

Console# show version

Console# show clock

Console# show history
```

---

show privilege

Use the **show privilege** privileged EXEC command to display the current privilege level.

Syntax

show privilege

Default Configuration

This command has no default configuration.

Command Mode

Privilege EXEC Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the current privilege level.

```
Console# show privilege

Current privilege level is 15
```

Back to Contents Page

Back to Contents Page

Using the CLI

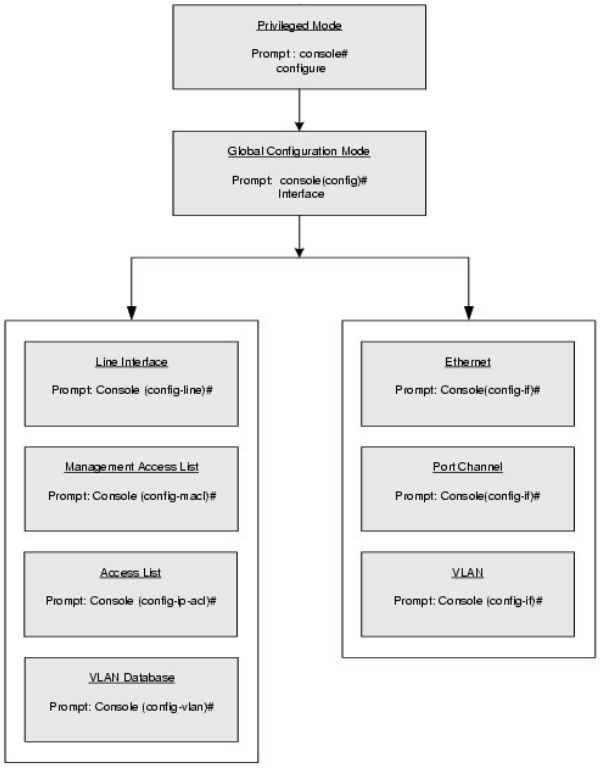
Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- CLI Command Modes
- Starting the CLI
- Editing Features

CLI Command Modes

To assist in configuring devices, the CLI command-line interface is divided into different command modes. Each command mode has its own set of specific commands. Entering a question mark ? at the system prompt (console prompt) displays a list of commands available for that particular command mode.

From each mode a specific command is used to navigate from one command mode to another. The standard order to access these modes is as follows: User EXEC Mode, Privileged EXEC Mode, Global Configuration Mode, Interface Configuration Mode. The following figure illustrates the command mode access path.



When starting a session, the User EXEC Mode is the initial mode. Only a limited subset of commands are available in User EXEC Mode. This level is reserved for tasks that do not change the configuration. To enter the next level, the Privileged EXEC Mode, a password is required.

The Privileged EXEC Mode gives access to commands that are restricted on EXEC Mode and provides access to the device Configuration Mode.

The Global Configuration Mode manages the device configuration on a global level. For specific interface configurations, enter the next level, the Interface Configuration Mode.

The Interface Configuration Mode configures specific interfaces in the device.

User EXEC Mode

After logging on to the device, the user is automatically in User EXEC command mode unless the user is defined as a privileged user. In general, the User EXEC commands allow the user to perform basic tests, and list system information.

The user-level prompt consists of the device host name followed by the angle bracket (>)

```
console>
```

The default host name is Console unless it has been changed using the **hostname** command in the Global Configuration Mode.

Privileged EXEC Mode

Because many of the privileged commands set operating parameters, privileged access is password protected to prevent unauthorized use. The password is not displayed on the screen and is case sensitive.

Privileged users are entered directly into the Privileged EXEC Mode. To enter the Privileged EXEC Mode commands from the User EXEC Mode, perform the following steps:

1. At the prompt enter the **enable** command and press <Enter>. A password prompt is displayed.

Enter the password and press <Enter>. The password is displayed as *. The privileged EXEC Mode prompt is displayed. The Privileged EXEC Mode prompt consists of the device host name followed by the pound sign #.

```
console#
```

To return from Privileged Mode to User EXEC Mode, use the **disable** command.

The following example illustrates how to access Privileged EXEC Mode and return to the User EXEC Mode:

```
console>enable

Enter Password: ******

console#

console#disable
 console>
```

The **exit** command is used to move back from any mode to a previous level mode, except from Privileged EXEC to User EXEC Mode, for example, from Interface Configuration Mode to Global Configuration Mode, and from Global Configuration Mode to Privileged EXEC Mode.

For more information about the **exit** command see exit(configuration), exit(EXEC), and end.

Global Configuration Mode

Global configuration commands apply to features that affect the system as a whole, rather than just a specific interface. The Privileged EXEC Mode command **configure** is used to enter the Global Configuration Mode.

The Global Configuration Mode commands perform the following:

1. At the Privileged EXEC Mode prompt, enter the command **configure** and press <Enter>. The Global Configuration Mode prompt is displayed. The Global Configuration Mode prompt consists of the device *host name* followed by the word (config) and pound sign #.

```
console(config)#
```

To return from Global Configuration Mode to Privileged EXEC Mode, use one of the following commands:

- **exit**
- **end**
- Ctrl+Z

The following example illustrates how to access Global Configuration Mode and return to the Privileged EXEC Mode:

```
console#

console#configure

console(config)#exit

console#
```

Interface Configuration Mode and Specific Configuration Modes

Interface Configuration commands modify specific IP interface operations such as a bridge-group, description, and so on. The five Interface Configuration Modes are as follows:

- **VLAN**—Contains commands to create an entire VLAN. The Global Configuration Mode command **vlan database** is used to enter the VLAN Interface Configuration Mode.
- **Port Channel**—Contains commands to configure port-channels, for example, assigning ports to a VLAN or port-channel. The Global Configuration Mode command interface port-channel is used to enter the port-channel Interface Configuration Mode.
- **Line Interface**—Contains commands to configure management connections such as line speed, timeout settings, and so on. The Global Configuration Mode command line is used to enter the line configuration command mode.
- **Management Access List**—Contains commands to define management access-lists for management. The Global Configuration Mode command **management access-list** is used to enter the Port Channel Interface Configuration Mode.
- **Ethernet**—Contains commands to manage port configuration. The Global Configuration Mode command interface ethernet enters the Interface Configuration Mode to configure an ethernet type interface

To access and list the VLAN Interface Configuration Mode commands, perform the following steps:

1. At the Global Configuration Mode prompt, enter the command `vlan database` and press <Enter>. The VLAN Interface Configuration Mode prompt is displayed. The VLAN Interface Configuration Mode prompt consists of the device *host name* followed by the word `(config-switch)` and the pound sign (#).

```
console(config-switch)#
```

2. Enter the ? command. The list of VLAN Interface Configuration Mode commands is displayed.

To access and list the port-channel Interface Configuration Mode commands, perform the following:

1. At the Global Configuration Mode prompt enter the command `interface port- channel port` channel-number and press <Enter>. The Interface Configuration Mode prompt is displayed. The Interface Configuration Mode prompt consists of the device *host name* followed by the word `(config-if)` and the pound sign (#).

```
console(config-if)#
```

Starting the CLI

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

If access is via a Telnet connection, ensure the device has an IP address defined and that the workstation used to access the device is connected to the device prior to using CLI commands.

Console Connection

To launch a command line window, perform the following steps:

1. Start the device and wait until the startup procedure is complete.
2. The User Exec Mode opens, and the Console> prompt is displayed.
3. Configure the device and enter the necessary commands to complete the required tasks.
4. When finished, type `quit` or `exit` to exit the session.

When a different user is required to log on to the system, enter the login command in the Privileged EXEC Mode. The current user is logged off and the new user is logged on.

Editing Features

Entering Commands

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/e5`, **show**, **interfaces,** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and `1/e5` specifies the unit/port.

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 smith`

Commands are entered manually on the CLI. To see the available commands for each Mode or within an Interface Configuration context, the CLI provides commands for displaying available commands, command syntax requirements and in some instances parameters required to complete the command. The standard command requesting help is the ?.

There are two instances where the help information can be displayed:

- **Keyword lookup**—Enter the character ? in place of a command. A list of all commands and corresponding help messages are displayed.
- **Partial keyword lookup**—If a command is incomplete and the character ? is entered in place of a parameter, the matched parameters for this command are displayed.

The CLI uses the following editing features:

- Terminal Command Buffer
- Command Completion
- Keyboard Shortcuts

Terminal Command Buffer

When a command is entered in the CLI, it is recorded on an internally managed Command History buffer. Commands are stored in the buffer, which is maintained on a First In First Out (FIFO) basis. These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved across device resets.

The following table describes commands to access the buffer:

Keyword	Source or destination
Up arrow key, Ctrl+P	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down arrow key	Returns to more recent commands in the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.

By default, the history buffer system is enabled, but it can be disabled at any time. For the command syntax to enable or disable the history buffer, see history.

There is a standard default number of commands that are stored in the buffer. The standard number of 10 commands can be increased to 256. By configuring 0, the effect is the same as disabling the history buffer system. For the command syntax on configuring the command history buffer, see history size.

To display the history buffer, see show history.

Negating the Effect of Commands

Many configuration commands use the prefix keyword **no** to cancel a command or reset the configuration to the default value. This guide describes the negation effect for all applicable commands.

Command Completion

When you type enough characters to identify a unique command, that command appears even if not complete. You can type the first few characters of a command to display all commands that begin with those characters. Press <Tab> repeatedly to move through the list to the correct command. For example, typing `history s` displays the command **history size**. Typing `history` displays the **history** and **history size** commands. To select **history size**, press <Tab> twice and then press <Enter>.

Incorrect or incomplete commands are automatically re-entered next to the cursor. If a parameter must be added, the parameter can be added to the basic command already displayed next to the cursor. The following example indicates that the command **interface ethernet** requires the parameter `<port-num>`.

```
(config)#interface ethernet

USAGE: interface ethernet <port-num>

port-num: The ethernet port

Mandatory parameter is omitted

(config)#interface ethernet
```

Keyboard Shortcuts

The CLI has a range of keyboard shortcuts to assist in editing the CLI commands. The following table describes the CLI shortcuts.

Keyboard Key	Description
Up arrow key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down arrow key	Returns to more recent commands in the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+z	Exits back to the next top level from all modes. For example, if in the Global Configuration Mode, exit back to the Privileged EXEC Mode.
Backspace key	Moves the cursor to the end of the command line.

CLI Command Conventions

The following table describes the command conventions for the CLI.

Convention	Description
[ ]	Indicates an optional entry.
{ }	Indicates a selection of compulsory parameters separated by the | character. One option must be selected. For example: **flowcontrol {auto|on|off}** means that for the **flowcontrol** command either **auto**, **on,** or **off** must be selected.
Italic font	Indicates a parameter.
<Enter>	Any individual key on the keyboard. For example click <Enter>.
Ctrl+F4	Any combination keys pressed simultaneously on the keyboard.
Screen Display	Indicates system messages and prompts appearing on the console.
#/g# or e#	Interface number corresponding to the following format: g for giga port or e for ethernet port.
all	When defining a range of ports or parameters, the default is **all** when no parameters are defined. For example, the command **interface range port-channel** has the option of either entering a range of channels, or selecting **all**. When the command is entered without a

	parameter, it automatically defaults to **all**.

Back to Contents Page

Back to Contents Page

VLAN Commands

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- vlan database
- vlan
- interface vlan
- interface range vlan
- name
- switchport mode
- switchport access vlan
- switchport trunk allowed vlan
- switchport trunk native vlan
- switchport general allowed vlan
- switchport general pvid
- switchport general ingress-filtering disable
- switchport general acceptable-frame-types tagged-only
- switchport forbidden vlan
- show vlan
- show interfaces switchport

---

vlan database

Use the **vlan database** global configuration command to enter the VLAN database configuration mode.

Syntax

vlan database

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters the VLAN database mode.

```
Console # vlan database

Console (config-vlan)#
```

---

vlan

Use the **vlan** interface configuration (VLAN) command to create a VLAN. To delete a VLAN, use the **no** form of this command.

Syntax

vlan {*vlan-range*}

no vlan {*vlan-range*}

- *vlan-range*—A list of VLAN IDs to be added. List separate, non-consecutive VLAN IDs separated by commas without spaces. A hyphen designates a range of IDs.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) Mode

User Guidelines

The maximum number of VLANs is **4095**.

Example

The following example creates VLAN number 1972.

```
Console # vlan database

Console (config-vlan)# vlan 1972
```

---

interface vlan

Use the **interface vlan** global configuration command to enter the interface configuration (VLAN) mode to configure an existing VLAN.

Syntax

interface vlan *vlan-id*

- *vlan-id*—The ID of an existing VLAN (excluding GVRP dynamic VLANs).

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the VLAN 1 IP address of 10.1.2.3 and subnet mask 255.0.0.0.

```
Console (config)# interface vlan 1

Console (config-if)# ip address 10.1.2.3 255.0.0.0
```

---

interface range vlan

Use the **interface range vlan** global configuration command to enter the interface configuration (VLAN) mode with the specified VLAN-list as the context.

Syntax

interface range vlan { *vlan-range* | **all** }

- *vlan-range*—A list of VLAN IDs to add. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **all**—All existing static VLANs.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

Commands under the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, an error message is displayed and execution continues on other interfaces.

Example

The following example groups VLAN 221-228 and VLAN 889 to receive the same command.

```
Console (config)# interface range vlan 221-228, 889

Console (config-if)#
```

---

name

Use the **name** interface configuration command to add a name to a VLAN. To remove the VLAN name, use the **no** form of this command.

Syntax

name *string*

no name

- *string*—A VLAN name, up to 32 characters in length.

Default Configuration

No name is defined.

Command Mode

Interface Configuration (VLAN) Mode

User Guidelines

The VLAN name should be unique.

Example

The following example names VLAN interface 19 as Marketing.

```
Console (config)# interface vlan 19

Console (config-if)# name Marketing
```

---

switchport mode

Use the **switchport mode** interface configuration command to configure a port VLAN membership mode. To reset the mode to the appropriate default for the port, use the **no** form of this command.

Syntax

switchport mode { **access** | **trunk** | **general** }

no switchport mode

- **access**—Port belongs to a single, untagged VLAN.
- **trunk**—Port belongs to 1...n VLANs, all tagged (except, optionally, for a single native VLAN).
- **general**—Port belongs to 1...n VLANs, and each VLAN is explicitly set by the user as tagged or untagged (full 802.1Q mode).

Default Configuration

All ports are in access mode and belong to the default VLAN (whose VID=1).

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures port 1/e8 as an untagged layer 2 VLAN interface.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# switchport mode access
```

---

switchport access vlan

The **switchport access vlan** interface configuration command configures the VLAN ID when the interface is in access mode. To reconfigure the default, use the **no** form of this command.

Syntax

switchport access vlan *vlan-id*

no switchport access vlan

- *vlan-id*—VLAN ID to which the port is configured.

Default Configuration

The default VLAN ID is **1**.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

The command automatically removes the port from the previous VLAN, and adds it to the new VLAN.

Example

The following example configures a VLAN ID of 23 to the untagged layer 2 VLAN interface number 1/e8.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# switchport mode access

console (config-if)# switchport access vlan 23
```

---

switchport trunk allowed vlan

Use the **switchport trunk allowed vlan** interface configuration command to add or remove VLANs from a trunk port.

Syntax

switchport trunk allowed vlan {**add** *vlan-list* | **remove** *vlan-list*}

- **add** *vlan-list*—List of VLAN IDs to add. Separate non-consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove** *vlan-list*—List of VLAN IDs to remove. Separate non-consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example adds VLANs to the allowed list of port 1/e8.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# switchport mode trunk

Console (config-if)# switchport trunk allowed vlan add 1,2,5-8
```

---

switchport trunk native vlan

Use the **switchport trunk native vlan** interface configuration command to define the port as a member of the specified VLAN, and the VLAN ID as the port default VLAN ID (PVID). To configure the default VLANID, use the **no** form of this command.

Syntax

switchport trunk native vlan *vlan-id*

no switchport trunk native vlan

- *vlan-id*—A VLAN ID for the active VLAN.

Default Configuration

The default VLAN ID is **1**.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

Incoming untagged frames are assigned to this VLAN and outgoing traffic from this VLAN is sent untagged (despite the normal situation where traffic sent from a trunk-mode port is all tagged).

The port is added as a member in the VLAN. If the port is already a member in the VLAN (not as a native), it should be removed from the VLAN first.

Example

The following example defines port 1/e8, in trunk mode, and is configured to use VLAN number 123 as the native VLAN.

```
console (config)# interface ethernet 1/e8

Console (config-if)# switchport mode trunk

console (config-if)# switchport trunk native vlan 123
```

---

switchport general allowed vlan

Use the **switchport general allowed vlan** interface configuration command to add and remove VLANs from a port in general mode.

Syntax

switchport general allowed vlan add *vlan-list* [**tagged** | **untagged**]

switchport general allowed vlan remove *vlan-list*

- **add** *vlan-list*—List of VLAN IDs to add. Separate non-consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove** *vlan-list*—List of VLAN IDs to remove. Separate non-consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **tagged**—Sets the port to transmit tagged packets for the VLANs. If the port is added to a VLAN without specifying tagged or untagged, the default is **tagged**.
- **untagged**—Set the port to transmit untagged packets for the VLANs.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to add VLANs to the allowed list.

```
console (config)# interface ethernet 1/e8

Console (config-if)# switchport mode general

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

---

switchport general pvid

Use the **switchport general pvid** interface configuration command to configure the Port VLAN ID (PVID) when the interface is in general mode. To configure the default value, use the **no** form of this command.

Syntax

switchport general pvid *vlan-id*

no switchport general pvid

- *vlan-id*—PVID. The VLAN ID may belong to a non-existent VLAN.

Default Configuration

The default VLAN ID is **1**.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the PVID for port 1/e8, when the interface is in general mode.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# switchport mode general

Console (config-if)# switchport general pvid 234
```

---

switchport general ingress-filtering disable

Use the **switchport general ingress-filtering disable** interface configuration command to disable port ingress filtering. To enable ingress filtering on a port, use the **no** form of this command.

Syntax

switchport general ingress-filtering disable

no switchport general ingress-filtering disable

Default Configuration

Ingress filtering is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example disables port ingress filtering on port 1/e8.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# switchport general ingress-filtering disable
```

---

switchport general acceptable-frame-types tagged-only

Use the **switchport general acceptable-frame-types tagged-only** interface configuration command to discard untagged frames at ingress. To enable untagged frames at ingress, use the **no** form of this command.

Syntax

switchport general acceptable-frame-types tagged-only

no switchport general acceptable-frame-types tagged-only

Default Configuration

All frame types are accepted at ingress.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures port 1/e8 to discard untagged frames at ingress.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# switchport general acceptable-frame-types tagged-only
```

---

switchport forbidden vlan

Use the **switchport forbidden vlan** interface configuration command to forbid adding specific VLANs to a port. This command prevents GVRP from automatically making these VLANs active on the selected ports. To allow the addition of specific VLANs to the port, use the **no** form of this command.

Syntax

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}

- **add** *vlan-list*—List of VLAN IDs to add to the forbidden list. Separate non-consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove** *vlan-list*—List of VLAN IDs to remove from the forbidden list. Separate non-consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

Default Configuration

All VLANs are allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example forbids adding VLANs 234-256 to port 1/e8.

```
Console (config)# interface ethernet 1/e8

Console (config-if)# switchport forbidden vlan add 234-256
```

---

show vlan

Use the **show vlan** privileged EXEC command to display VLAN information.

Syntax

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

- *vlan-id*—A configured VLAN ID.
- *vlan-name*—A VLAN name string (Range: **1-32** characters).

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all VLAN information.

```
Console# show vlan

VLAN Name Ports Type

-------- --------------- ------ -----

1 default 1/e1-2 Other

2/e1-4

10 VLAN0010 1/e3-4 dynamic

11 VLAN0011 1/e1-2 permanent

20 VLAN0020 1/e3-4 permanent

21 VLAN0021 permanent

30 VLAN0030 permanent

31 VLAN0031 permanent
```

show interfaces switchport

Use the **show interfaces switchport** privileged EXEC command to display switchport configuration.

Syntax

show interfaces switchport {**ethernet** *interface* | **port-channel** *port-channel-number*}

- *interface*—Specific interface, such as ethernet 1/e8.
- *port-channel-number*—A port-channel trunk Index

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC Mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays switchport configuration for port 1/e1.

```
Console# show interface switchport ethernet 1/e1

Port 1/e1:

VLAN Membership mode: General

PVID: 1 (default)

Ingress Filtering: Enabled

Acceptable Frame Type: All

GVRP status: Enabled
```

```
Port 1/e1 is member in:

VLAN Name Egress rule

---- --------- -----------

1 default untagged

8 VLAN008 untagged

11 VLAN0011 tagged

19 IPv6 VLAN untagged

72 VLAN0072 untagged



Forbidden VLANS:

VLAN Name

---- ---------

73 Out



Classification rules:

Protocol Group VLAN

-------------- ----

2 19

3 72
```

Back to Contents Page

Back to Contents Page

Web Server

Dell™ PowerConnect™ 3324/3348 Switch CLI Guide

- ip http port
- ip http server
- ip https port
- ip https server
- crypto certificate generate
- show ip http
- show ip https

---

ip http port

Use the **ip http port** global configuration command to specify the TCP port for use by a web browser to configure the device. To use the default TCP port, use the **no** form of this command.

Syntax

ip http port *port-number*

no ip http port

- *port-number*—Port number for use by the HTTP server (Range: **0-65535**).

Default Configuration

This default port number is **80**.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example configures the http port number to 100.

```
Console (config)# ip http port 100
```

---

ip http server

Use the **ip http server** global configuration command to enable the device to be configured from a browser. To disable this function, use the **no** form of this command.

Syntax

ip http server

no ip http server

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example enables the device to be configured from a browser.

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

---

ip https port

Use the **ip https port** global configuration command to configure a TCP port for use by a secure web browser to configure the device. To use the default port, use the **no** form of this command.

Syntax

ip http ports *port-number*

no ip http ports

- *port-number*—Port number for use by the HTTP server (Range: **0-65535**).

Default Configuration

This default port number is **443**.

Command Mode

Global Configuration Mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example configures the https port number to 100.

```
Console (config)# ip https port 100
```

---

ip https server

Use the **ip https server** global configuration command to enable the device to be configured from a secured browser. To disable this function, use the **no** form of this command.

Syntax

ip https server

no ip https server

Default Configuration

The default is the device that is enabled to be configured from a browser.

Command Mode

Global Configuration Mode

User Guidelines

console(config)# crypto certificate generate key_generate

Examples

The following example enables the device to be configured from a browser.

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

---

crypto certificate generate

Use the **crypto certificate generate** global configuration command to generate a HTTPS certificate.

Syntax

crypto certificate generate [**key-generate** [*length*]]

- **key-generate**—Regenerate SSL RSA key.
- *length*—Specifies the SSL RSA key length. If unspecified, the default is 1024.

Default Configuration

The Certificate and the SSL RSA key pairs do not exist.

Command Mode

Global Configuration Mode

User Guidelines

The command is not saved in the device configuration; however, the certificate and keys generated by this command are saved in the private configuration (which is never displayed to the user or backed up to another device).

Examples

The following example regenerates an HTTPS certificate.

```
Console (config)# crypto certificate generate key-generate

Generating RSA private key, 1024 bit long modules
```

```
Console (config)#
```

---

show ip http

Use the **show ip http** privileged EXEC command to display the HTTP server configuration.

Syntax

show ip http

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC command

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the HTTP server configuration.

```
Console# show ip http

HTTP server enabled. Port: 80
```

---

show ip https

Use the **show ip http** privileged EXEC command to display the HTTPS server configuration.

Syntax

show ip https

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC command

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the HTTP server configuration.

```
Console# show ip https

HTTPS server enabled. Port: 443

Certificate was generated.
```

Back to Contents Page